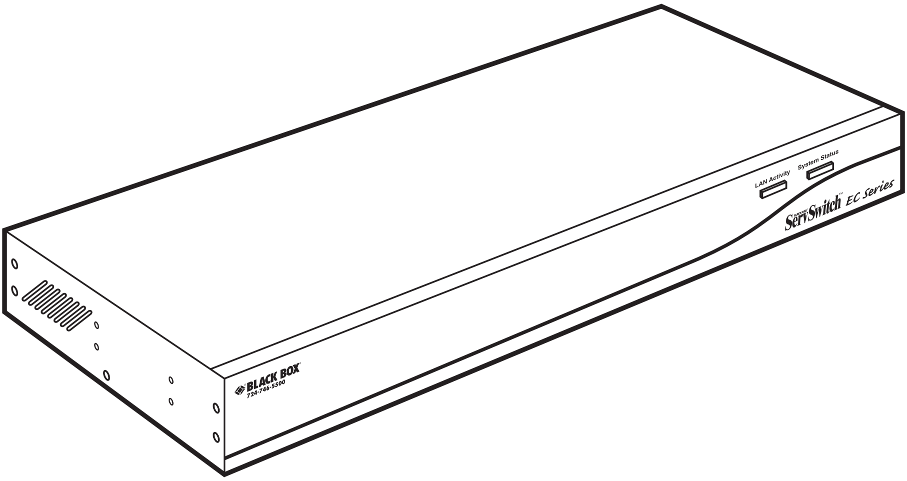
BLACK BOX®
NETWORK SERVICES

1000 Park Drive • Lawrence, PA 15055-1018 • 724-746-5500 • Fax 724-746-0746

MAY 2007
KV9304A-R2
KV9308A-R2
KV9316A-R2

4-, 8-, and 16-Port ServSwitch EC Series IP KVM Switch



CUSTOMER
SUPPORT
INFORMATION

Order **toll-free** in the U.S.: Call **877-877-BBOX** (outside U.S. call **724-746-5500**)
FREE technical support 24 hours a day, 7 days a week: Call **724-746-5500** or fax **724-746-0746**
Mailing address: **Black Box Corporation**, 1000 Park Drive, Lawrence, PA 15055-1018
Web site: **www.blackbox.com** • E-mail: **info@blackbox.com**

FEDERAL COMMUNICATIONS COMMISSION
AND
INDUSTRY CANADA
RADIO FREQUENCY INTERFERENCE STATEMENTS

Class B Digital Device. This equipment has been tested and found to comply with the limits for a Class B computing device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation. This equipment generates, uses, and can radiate radio frequency energy, and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. If this equipment does cause harmful interference to radio or telephone reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult an experienced radio/TV technician for help.

CAUTION

Changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment.

To meet FCC requirements, shielded cables and power cords are required to connect this device to a personal computer or other Class B certified device.

This digital apparatus does not exceed the Class B limits for radio noise emission from digital apparatus set out in the Radio Interference Regulation of Industry Canada.

Le présent appareil numérique n’émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de classe B prescrites dans le Règlement sur le brouillage radioélectrique publié par Industrie Canada.

NORMAS OFICIALES MEXICANAS (NOM)
ELECTRICAL SAFETY STATEMENT

INSTRUCCIONES DE SEGURIDAD

1. Todas las instrucciones de seguridad y operación deberán ser leídas antes de que el aparato eléctrico sea operado.

2. Las instrucciones de seguridad y operación deberán ser guardadas para referencia futura.

3. Todas las advertencias en el aparato eléctrico y en sus instrucciones de operación deben ser respetadas.

4. Todas las instrucciones de operación y uso deben ser seguidas.

5. El aparato eléctrico no deberá ser usado cerca del agua—por ejemplo, cerca de la tina de baño, lavabo, sótano mojado o cerca de una alberca, etc..

6. El aparato eléctrico debe ser usado únicamente con carritos o pedestales que sean recomendados por el fabricante.

7. El aparato eléctrico debe ser montado a la pared o al techo sólo como sea recomendado por el fabricante.

8. Servicio—El usuario no debe intentar dar servicio al equipo eléctrico más allá a lo descrito en las instrucciones de operación. Todo otro servicio deberá ser referido a personal de servicio calificado.

9. El aparato eléctrico debe ser situado de tal manera que su posición no interfiera su uso. La colocación del aparato eléctrico sobre una cama, sofá, alfombra o superficie similar puede bloquea la ventilación, no se debe colocar en libreros o gabinetes que impidan el flujo de aire por los orificios de ventilación.

10. El equipo eléctrico deber ser situado fuera del alcance de fuentes de calor como radiadores, registros de calor, estufas u otros aparatos (incluyendo amplificadores) que producen calor.

11. El aparato eléctrico deberá ser connectado a una fuente de poder sólo del tipo descrito en el instructivo de operación, o como se indique en el aparato.

12. Precaución debe ser tomada de tal manera que la tierra fisica y la polarización del equipo no sea eliminada.

13. Los cables de la fuente de poder deben ser guiados de tal manera que no sean pisados ni pellizcados por objetos colocados sobre o contra ellos, poniendo particular atención a los contactos y receptáculos donde salen del aparato.

14. El equipo eléctrico debe ser limpiado únicamente de acuerdo a las recomendaciones del fabricante.

15. En caso de existir, una antena externa deberá ser localizada lejos de las lineas de energia.

16. El cable de corriente deberá ser desconectado del cuando el equipo no sea usado por un largo periodo de tiempo.

17. Cuidado debe ser tomado de tal manera que objectos liquidos no sean derramados sobre la cubierta u orificios de ventilación.

18. Servicio por personal calificado deberá ser provisto cuando:

    A: El cable de poder o el contacto ha sido dañado; u

    B: Objectos han caído o líquido ha sido derramado dentro del aparato; o

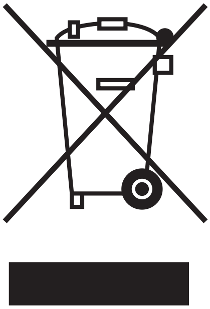
    C: El aparato ha sido expuesto a la lluvia; o

    D: El aparato parece no operar normalmente o muestra un cambio en su desempeño; o

    E: El aparato ha sido tirado o su cubierta ha sido dañada.

RoHS Compliance

The ServSwitch EC Series IP KVM Switch is RoHS compliant.



TRADEMARKS USED IN THIS MANUAL

Mac OS is a registered trademark of Apple Computer, Inc.

ServSwitch is a trademark, and BLACK BOX and the Double Diamond logo are registered trademarks of BB Technologies, Inc.

Hayes is a registered trademark of Hayes Microcomputer Products, Inc.

PS/2 is a registered trademark of International Business Machines Corporation.

Linux is a registered trademark of Linus Torvalds.

Windows is a registered trademark of Microsoft Corporation.

Java is a trademark, and JavaScript, Solaris, Sun, and Sun Microsystems are registered trademarks of Sun Microsystems, Inc.

UL is a registered trademark of Underwriters' Laboratories, Inc.

UNIX is a registered trademark of UNIX System Laboratories, Inc. (or USL).

Any other trademarks mentioned in this manual are acknowledged to be the property of the trademark owners.

Contents

Chapter **Page**

Contents (continued)

Chapter **Page**

Chapter **Page**

1. Specifications

Color Depth Adjustments: 8, 12, 16 bits selectable

Color Depth (Maximum): 16 bits

Supported Video Mode (Maximum): Local: 1600 x 1200 @ 85 Hz;
Remote: 1280 x 1024 @ 85 Hz (16-bit color)

User Controls: (1) IP Setup button, (1) dual-function Reset button (Power Reset, Restore to Factory Defaults)

Connectors: All: (1) barrel connector for power, (1) 8-pin mini-DIN (reserved for future use), (1) DB9 COM/RS-232 male, (1) HD15 for console video, (1) RJ-45 LAN, (2) 6-pin mini-DIN for console keyboard and mouse;
KV9304A-R2: (4) HD15 female integrated KVM cable input;
KV9308A-R2: (8) HD15 female integrated KVM cable input, (1) R-port (for serial device management with KV9-SRL);
KV9316A-R2: (16) HD15 female integrated KVM cable input, (1) R-port (for serial device management with KV9-SRL)

Indicators: (4) LEDs: (1) LAN Activity, (1) System Status, (1) Eth Act, (1) Sys OK

Power: 12-VDC power supply; maximum power consumption: 18 watts

Size: KV9304A-R2: 1.7"H x 7.3"W x 8.7"D (4.3 x 18.5 x 22.1 cm);
KV9308A-R2, KV9316A-R2: 1.7"H x 15.9"W x 8.7"D (4.3 x 40.4 x 22.1 cm)

2. Overview

2.1 Introduction

The 4-, 8-, and 16-Port ServSwitch™ EC Series IP KVM Switches allow you to use the Internet or your TCP/IP-enabled network to remotely monitor and control critical PC servers and workstations using an industry-standard Web browser or VNC client. Or, use On-Screen Display (OSD) or hotkeys to manage the switch. The ServSwitch is RoHS compliant. It features 16 bits of color depth that supports up to 65,536 colors.

The ServSwitch supports industry-standard networking and management protocols such as TCP/IP and SNMP. It offers secure management options including SSL encryption, SSH tunneling, and RADIUS. The ServSwitch is platform-independent and can be managed using any Java™ enabled Web browser.

2.2 Components

2.2.1 Front Panel

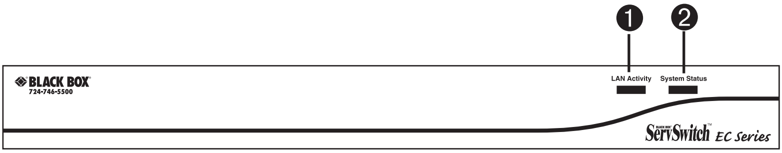


Figure 2-1. ServSwitch front-panel view.

Table 2-1. Front-panel components.

Component		Description
❶	LAN Activity LED	Lights when the LAN is active.
❷	System Status LED	Lights when the system is OK.

2.2.2 Back Panel

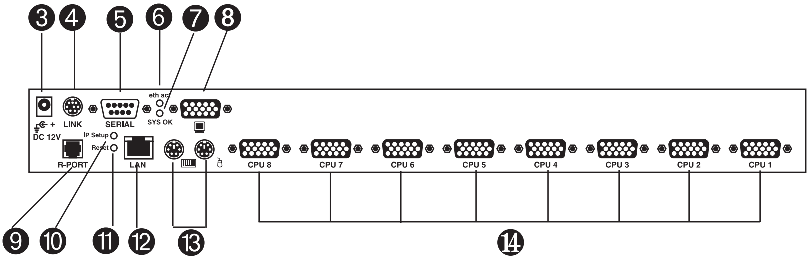


Figure 2-2. The 8-Port ServSwitch back-panel view.

Table 2-2. Rear-panel components.

Component		Description
❸	Barrel connector	Connects to a 12-VDC power adapter.
❹	8-pin mini-DIN connector	Reserved for future use.
❺	DB9 COM/RS-232 connector	Connects to a PC for initial setup only.
❻	Eth Act LED	Lights when the network is active.
❼	Sys OK LED	Lights when the network is on.
❽	HD15 connector	Connect to the shared console monitor.
❾	R-port (KV9308A-R2 and KV9316A-R2 only)	For serial device management with KV9-SRL.
❿	IP Setup button	Press this button with a paper clip or pen to bring up the IP-OSD menu.
⓫	Reset button	This dual-function button selects Power Reset or Restore Factory Defaults.
⓬	RJ-45 connector	Links to the LAN.
⓭	6-pin mini-DIN connectors	Connect to the shared console keyboard and mouse ports.

Table 2-2 (continued). Rear-panel components.

Component	Description
⓮ HD15 connectors	Connect to 4, 8, or 16 servers.

2.3 What's Included

Your package should include the following items. If anything is missing or damaged, contact Black Box at 724-746-5500.

- (1) 4-, 8-, or 16-Port ServSwitch EC Series IP KVM Switch
- (1) Power adapter
- (1) AC cord for power adapter
- (2) rackmount brackets
- (1) package of screws
- (1) set of foot pads
- (1) DB9 RS-232 null-modem serial cable
- This user's manual

2.4 Cables You'll Need to Supply

ServSwitch 3-in-1 Cable (EHN70001-0006, EHN70001-0010, EHN9000P-0015, or EHN9000P-0030): These cables connect to PCs that have an HD15 monitor connector and PS/2® keyboard and mouse connectors. The cables are available in 6-, 10-, 15-, and 30-foot (1.8-, 3-, 4.5-, and 9.1-m) versions.

ServSwitch 2-in-1 Cable (EHN9000U-0006, EHN9000U-0010, or EHN9000U-0015): These cables connect to PCs that have HD15 monitor and USB keyboard and mouse connectors. The cables are available in 6-, 10-, and 15-foot (1.8-, 3-, and 4.5-m) versions.

3. Installation

3.1 Quick Start Guide

This quick start guide describes two different ways to quickly set up your ServSwitch. These are described in **Sections 3.1.1** and **3.1.2**.

Before doing the initial setting:

1. Record your original computer settings, such as TCP/IP, in case you would like to use this computer for other tasks.

2. Make sure you have the latest Java software downloaded from *http://www.java.com.*

3. Disable mouse acceleration on the host computer(s) and client computer. See **Section 3.2** for details.

3.1.1 Using the IP-OSD Step-by-Step Menu (Recommended)

Hardware needed:

- (1) 4-, 8-, or 16-Port ServSwitch EC Series IP KVM Switch with a power adapter

- (1) keyboard and monitor

- (1) CAT5 cable with RJ-45 connector

1. Connect a PS/2 keyboard and monitor to the ServSwitch unit's local port.

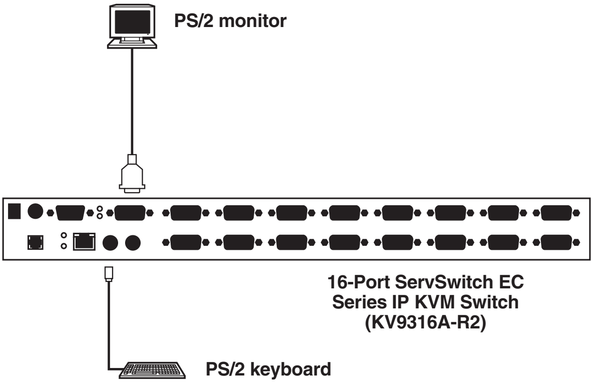


Figure 3-1. Connecting a PS/2 keyboard and monitor to the ServSwitch.

2. Connect a CAT5 cable to the ServSwitch unit's LAN port. Connect the other end of the cable to an Ethernet switch.

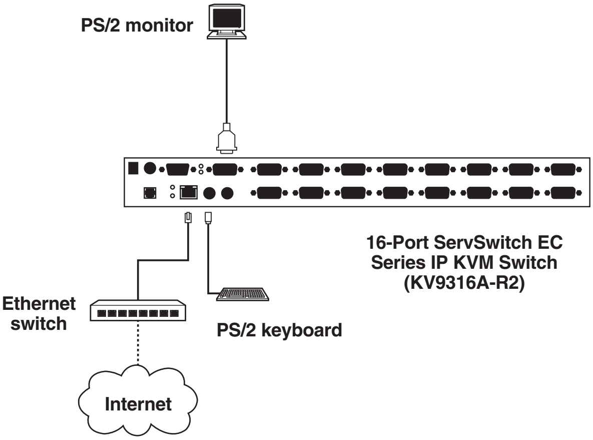


Figure 3-2. Connecting the ServSwitch to the Internet.

3. Power on the monitor and the ServSwitch. Using a paper clip or pen, press the IP Setup button located on the ServSwitch unit's back panel. Simply follow the step-by-step instructions to finish the initial setup.

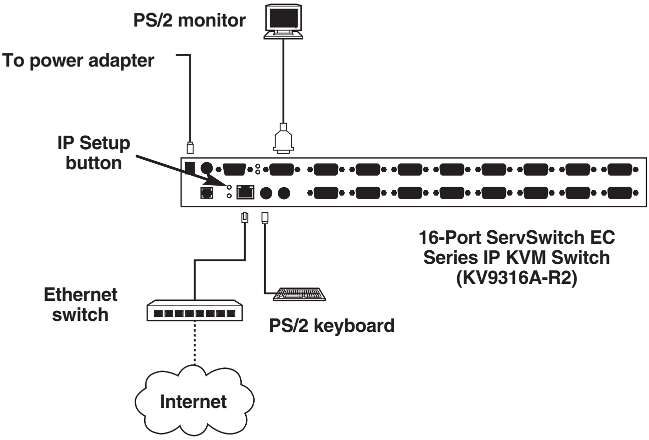
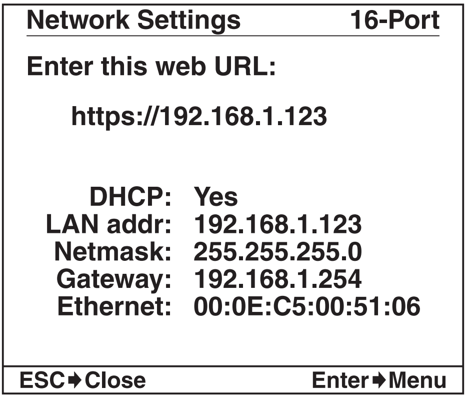


Figure 3-3. Connecting the power.

The Network Settings screen appears as shown in Figure 3-4.



```
Network Settings              16-Port

Enter this web URL:

    https://192.168.1.123


      DHCP:  Yes
  LAN addr:  192.168.1.123
   Netmask:  255.255.255.0
   Gateway:  192.168.1.254
  Ethernet:  00:0E:C5:00:51:06

ESC➔Close                  Enter➔Menu
```

Figure 3-4. Network Settings screen.

3.1.2 Using the HyperTerminal via a Serial Port

Hardware needed:

- (1) 4-, 8-, or 16-Port ServSwitch EC Series IP KVM Switch with a power adapter
- (1) computer with a keyboard, mouse, and monitor
- (1) DB9 RS-232 null-modem serial cable (included)

1. Connect the DB9 RS-232 null-modem serial cable to the serial port on the ServSwitch unit's rear panel. Connect the opposite end of the cable to the computer's serial port (COM1, COM2, etc.). See Figure 3-5.

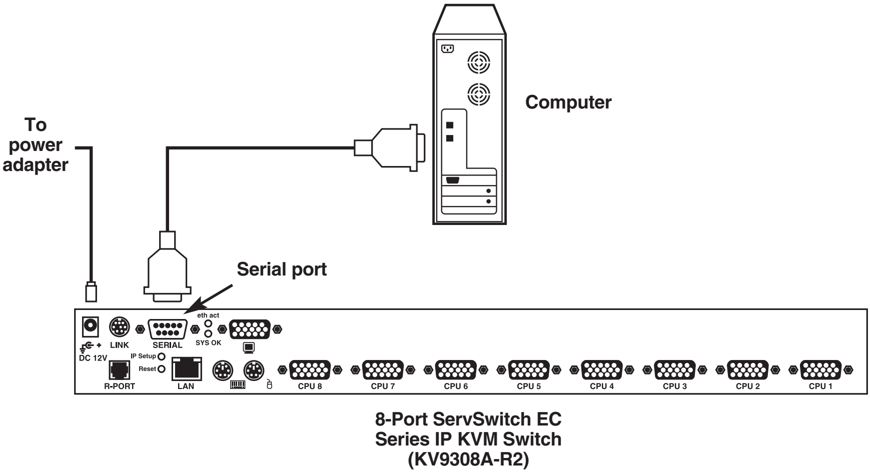


Figure 3-5. Connecting a computer to the ServSwitch unit's serial port.

2. From your computer's Administrator screen in Windows® XP, select **All Programs**, **Accessories**, **Communications**, and **HyperTerminal**. See Figure 3-6.

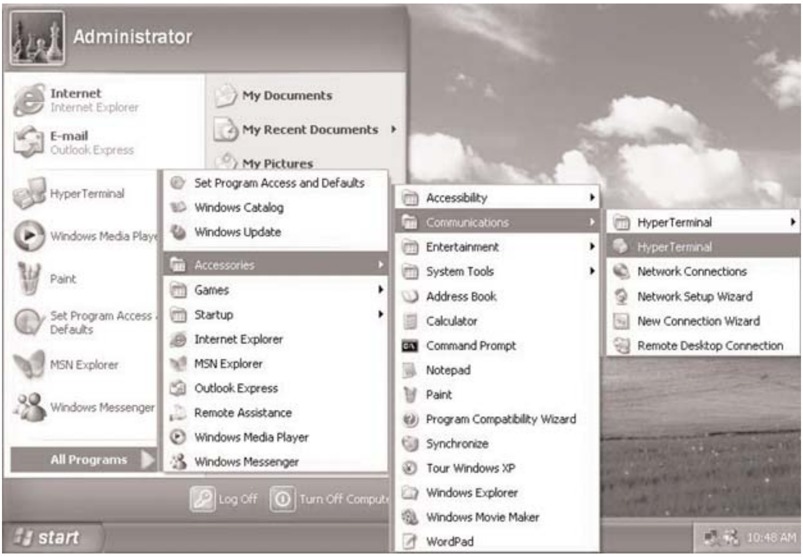
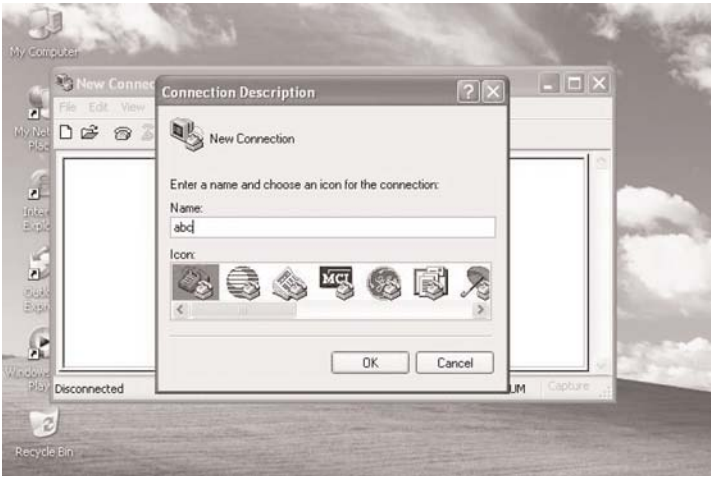


Figure 3-6. Administrator screen.

3. If you've never set up your HyperTerminal before, it will ask you to enter your phone area code. Enter this, then click on **OK**. The screen shown in Figure 3-7 appears.



Connection Description

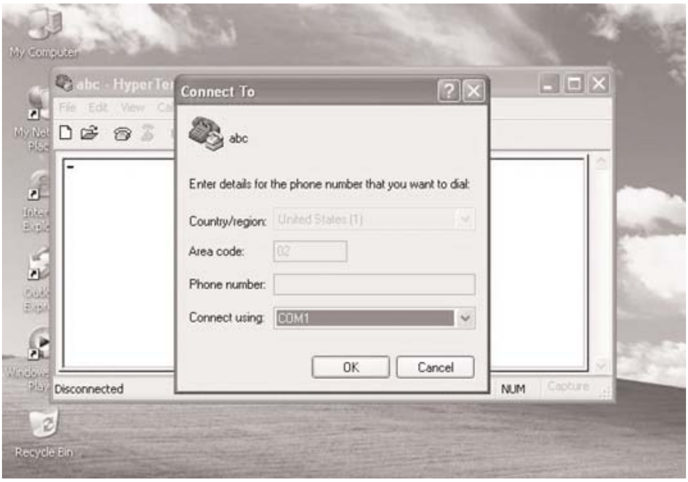
New Connection

Enter a name and choose an icon for the connection:

Name: abc

Figure 3-7. Connecting to HyperTerminal.

4. In the Name field, type in a name (for example, `abc`). Next, click on an icon to correspond to the chosen name. Then click on **OK**, or click on **Cancel** to type in a different name and/or select a different icon. If you click on **OK**, Figure 3-8 appears.



Connect To

abc

Enter details for the phone number that you want to dial:

Country/region: United States (1)

Area code: 02

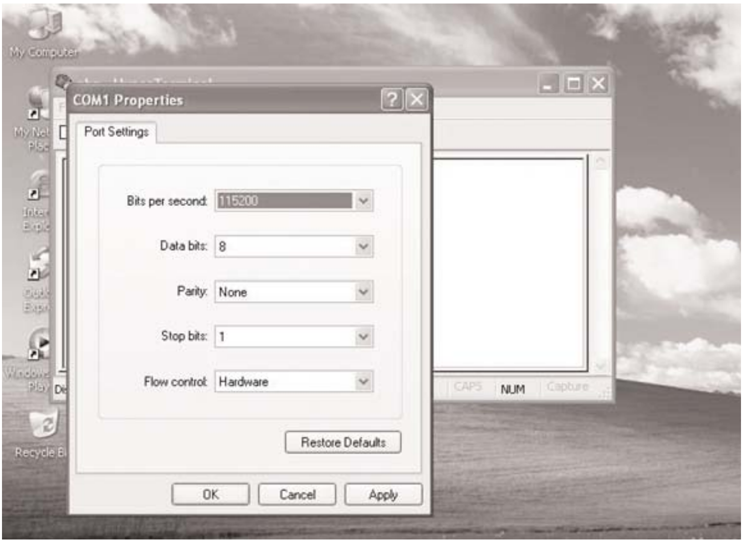
Phone number:

Connect using: COM1

Figure 3-8. Selecting the port.

5. From the Connect using drop-down menu, select the serial port that you want to connect (for example, COM1). Click on **OK** to save or **Cancel** to cancel.

6. If you click on **OK** in Figure 3-8, the screen shown in Figure 3-9 appears.



COM1 Properties

Port Settings

Bits per second: 115200

Data bits: 8

Parity: None

Stop bits: 1

Flow control: Hardware

Figure 3-9. Port Settings screen.

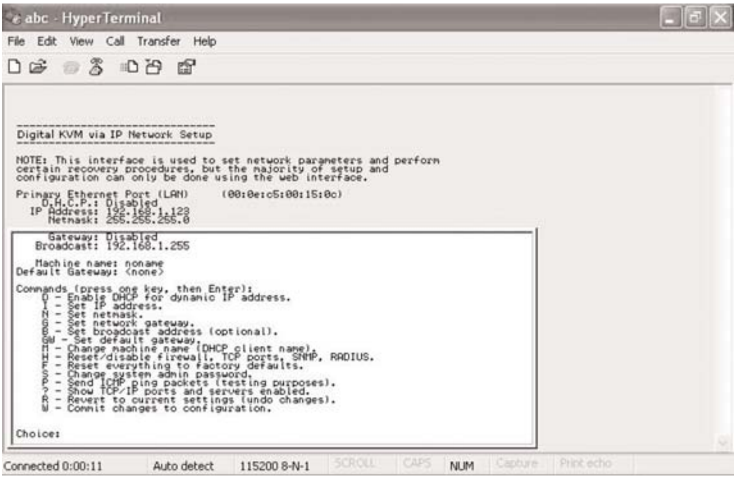
7. From the Bits per second drop-down menu, select 115200. Choose settings for data bits, parity, stop bits, and flow control from their respective drop-down menus. The default values are:

   Data bits: 8
   Parity: None
   Stop bits: 1
   Flow control: Hardware

   If you change any of these values, you can click on **Restore Defaults** to return to these values.

   Click **Cancel** to cancel the changes, **Apply** to apply the changes, or **OK** to save the changes.

8. If you click on **OK** in Figure 3-9, the screen shown in Figure 3-10 appears.



```
------------------------------------
Digital KVM via IP Network Setup
------------------------------------

NOTE: This interface is used to set network parameters and perform
certain recovery procedures, but the majority of setup and
configuration can only be done using the web interface.

Primary Ethernet Port (LAN)     (00:0e:c5:00:15:0c)
     D.H.C.P.: Disabled
   IP Address: 192.168.1.123
      Netmask: 255.255.255.0
      Gateway: Disabled
    Broadcast: 192.168.1.255

    Machine name: noname
Default Gateway: <none>

Commands (press one key, then Enter):
     D - Enable DHCP for dynamic IP address.
     I - Set IP address.
     N - Set netmask.
     G - Set network gateway.
     B - Set broadcast address (optional).
     GW - Set default gateway.
     M - Change machine name (DHCP client name).
     H - Reset/disable firewall, TCP ports, SNMP, RADIUS.
     F - Reset everything to factory defaults.
     S - Change system admin password.
     P - Send ICMP ping packets (testing purposes).
     ? - Show TCP/IP ports and servers enabled.
     R - Revert to current settings (undo changes).
     W - Commit changes to configuration.

Choice:
```

Figure 3-10. HyperTerminal screen.

9. Follow the instructions on the screen. For example, simply type `I` to set your IP address, type `F` to reset everything back to factory defaults, and so on.

NOTE

Remember to type `W` after you make any changes.

3.2 Disabling the Mouse Acceleration on the Computers

Many operating systems offer a feature called mouse acceleration that allows the user to adjust the responsiveness of the cursor on the screen to physical movements of the mouse. While this is usually a beneficial interface enhancement, it can interfere with the ServSwitch unit's operation and should be disabled on the managed computers before you attempt a remote session. Follow the instructions in **Sections 3.2.1** through **3.2.4**, depending on your operating system, to disable mouse acceleration for the operating system installed on each managed computer.

3.2.1 Windows 98 and Windows 2000

1. From the Control Panel, click on **Mouse**.
2. From Mouse Properties, click on the **Motion** tab.
3. Make sure that the Pointer speed bar is centered and Acceleration is set to None.

3.2.2 Windows XP and Windows Server 2003

1. From the Control Panel, click on **Mouse**.
2. Go to **Pointer Options** and turn off **Enhance Pointer Precision**.
3. Make sure that the Pointer speed bar is centered.

3.2.3 Linux®, UNIX®, and X-Windows

Add this command to your xinitrc, xsession or other startup script:

```
xset m 0/0 0
```

3.2.4 Sun® Solaris®

Add this command to your xinitrc, xsession or other startup script:

```
xset m 1/1 0
```

3.3 How to Connect Your ServSwitch

A typical example of a ServSwitch setup is shown in Figure 3-11. Refer to this diagram and follow the instructions discussed next when installing the ServSwitch.

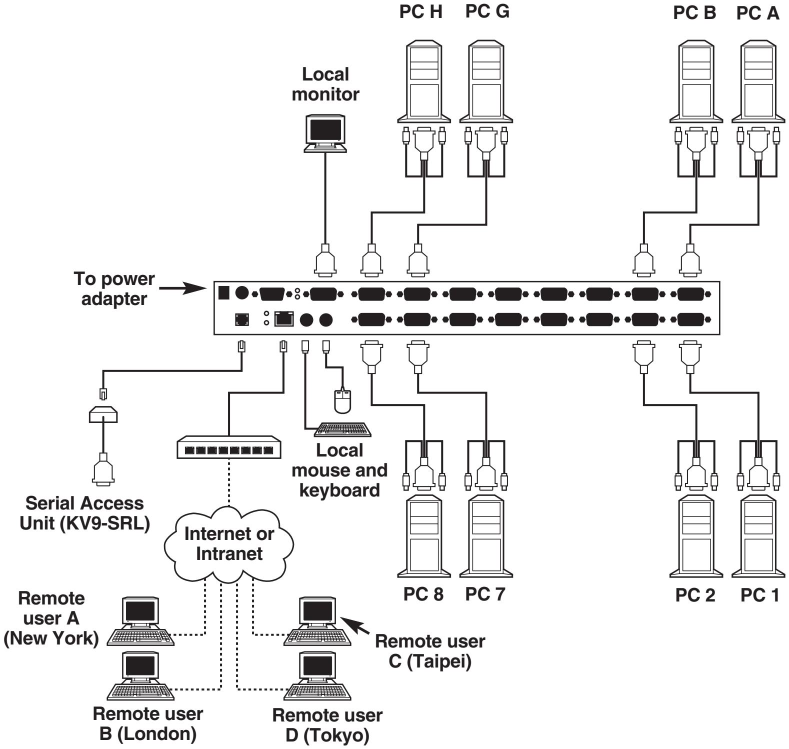


Figure 3-11. Sample setup using a 16-port ServSwitch (KV9316A-R2).

NOTE

The restrictions on functions such as cascading and the assignment of master and slave units apply to all ServSwitch versions.

1. Make sure that the ServSwitch and the computers to be managed are powered off.

2. If desired, mount the 4-, 8-, or 16-Port ServSwitch (KV9304A-R2, KV9308A-R2, or KV9316A-R2) in a standard rack or cabinet. Use the included rackmount brackets and screws. See Figure 3-12.

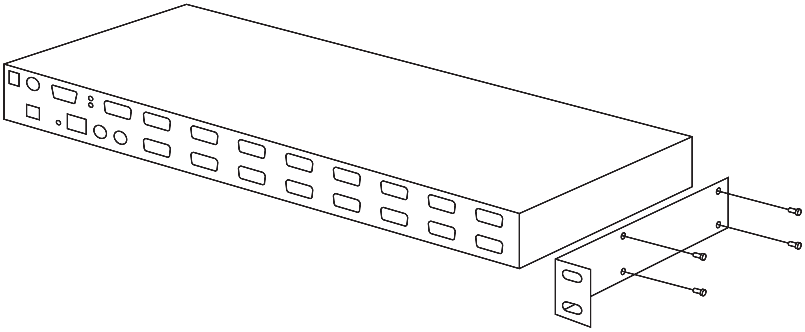


Figure 3-12. Rackmounting the ServSwitch.

3. Connect a straight-through Ethernet patch cable to the LAN port on the ServSwitch unit's rear panel.

4. Connect the opposite end of the cable to your network hub, switch, or terminated wall outlet.

5. If you want to use the ServSwitch as a local console, connect a standard keyboard (following the PC99 standard color codes) and mouse (also following the PC99 standard) as marked on the ServSwitch unit's rear panel.

6. Connect a VGA monitor to the video out port on the ServSwitch unit's rear panel.

7. If your managed computers (the computers are often servers or critical systems) have PS/2 connections, attach one end of a 3-in-1 Cable (EHN70001-0006, EHN70001-0010, EHN9000P-0015, or EHN9000P-0030) to the computer's available keyboard, mouse, and VGA out ports. Connect the opposite end of the cable (with a single HD15 VGA connector) to one of the PC 1–8 or PC A–H ports on the ServSwitch unit's rear panel. Repeat this procedure for each PS/2 enabled managed computer.

8. If your managed computers (the computers are often servers or other critical systems) have USB connections, attach one end of a 2-in-1 Cable (EHN9000U-0006, EHN9000U-0010, or EHN9000U-0015) to the computer's available USB port and video out port. Connect the opposite end of the cable (with a single HD15 VGA connector) to one of the PC 1–8 or PC A–H ports on the ServSwitch unit's rear panel. Repeat this procedure for each USB-enabled managed computer.

9. If you are using 1 to 16 optional Serial Access Units, connect the RJ-14 cable(s) (included with the Serial Access Unit[s], KV9-SRL) to the R-port on the ServSwitch unit(s).

10. Power on the ServSwitch by connecting the AC adapter to a suitable power outlet and the opposite end of the power cord to the 12-VDC port on the ServSwitch unit's rear panel.

11. Power on each of the managed computers, observing normal startup procedures.

NOTES

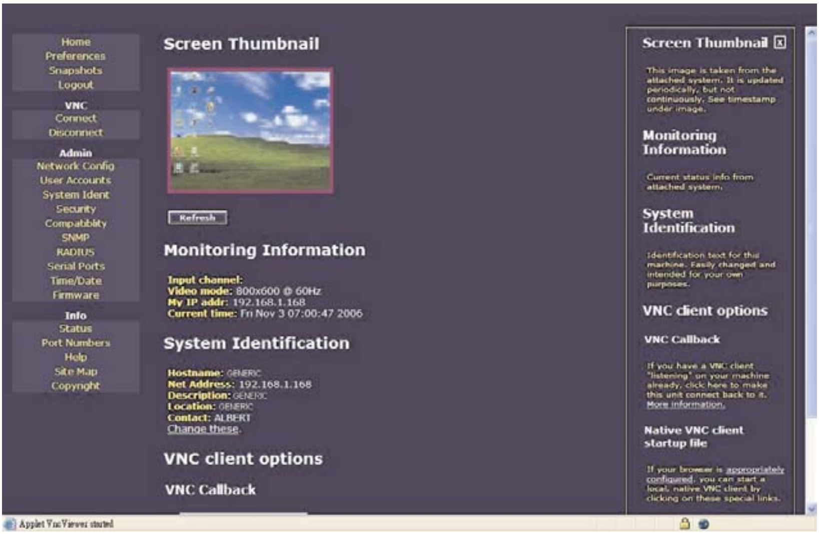
1. **You can choose to mix managed computers connected via PS/2 and USB connections as necessary with no impact on features or function.**

2. **Steps 5 and 6 are required only if you want to manage the ServSwitch and its computers locally (that is, not over the Internet or a LAN). While not required, we recommend adding these devices for easier administration.**

3. **You can cascade multiple ServSwitch units to increase the total number of possible managed computers. To take advantage of this feature, refer to Section 5.1.**

3.4 Access Your ServSwitch and Remotely Control the Host Computer(s)

As soon as you finish the settings and connections described in **Sections 3.1** through **3.3**, you are ready to remotely control the host computer(s). Simply open the Web browser and type in the IP you already set up in **Section 3.1**, then type in the correct username and password. Once you type the username and password, Figure 3-13 appears.



Screen Thumbnail

Monitoring Information

Input channel:
Video mode: 800x600 @ 60Hz
My IP addr: 192.168.1.168
Current time: Fri Nov 3 07:00:47 2006

System Identification

Hostname: GENERIC
Net Address: 192.168.1.168
Description: GENERIC
Location: GENERIC
Contact: ALBERT
Change these.

VNC client options

VNC Callback

Screen Thumbnail ☒

This image is taken from the attached system. It is updated periodically, but not continuously. See timestamp under image.

Monitoring Information

Current status info from attached system.

System Identification

Identification text for this machine. Easily changed and intended for your own purposes.

VNC client options

VNC Callback

If you have a VNC client "listening" on your machine already, click here to make this unit connect back to it. More information.

Native VNC client startup file

If your browser is appropriately configured, you can start a local, native VNC client by clicking on these special links.

Applet VncViewer started

Figure 3-13. Home screen.

Double-click on the small rectangle window in the middle of the screen shown in Figure 3-13. You'll get the VNC screen, which is the host computer's screen.

NOTE

You may need to upgrade or download your Java (*http://www.java.com*) support in your browser before using the VNC screen to remotely control the host computer(s). However, most modern browsers come with a version of Java that's compatible with this application.

From the VNC (host computer's) screen, you can control the host computer remotely just like you could if you were physically present at the host computer's location.

To log out, simply click on the **Logout** icon at the top of the screen.

4. Advanced Operations

The Web interface is the most intuitive way to configure the ServSwitch. It also offers a Java based VNC client that you can use to control the managed computers from a remote location. The ServSwitch supports any industry-standard HTML Web browser. To access the Web interface, open your Web browser and type in the IP address of the unit you wish to access/configure. The IP address will be either:

a) the address assigned for the LAN port by your DHCP server as identified in **Chapter 3**,

or

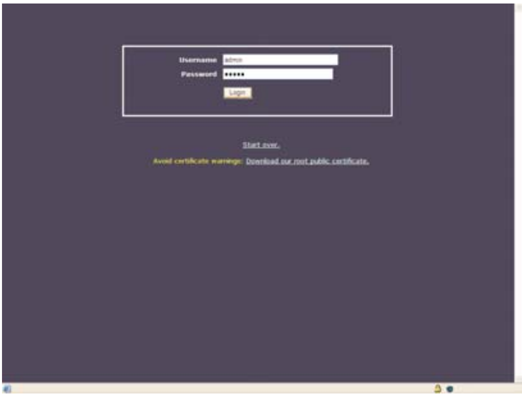
b) the fixed IP address you set up (see **Section 3.1** for more information). Again, the default IP address for the ServSwitch unit's LAN port is `https://192.168.1.123`.

4.1 How to Log in to the ServSwitch (the Home Screen)

1. Before you can access the Web configuration interface, you must type in a username and password. The default username and password as shipped from the factory is username `admin` with a password of `admin`. See Figure 4-1.

NOTE

Before the login screen appears, your Web browser may display a warning about an invalid security certificate. This does not affect the security of your data in any way. Whenever you are prompted about a certificate security problem by your browser or the Java VNC client, always choose the option to continue.



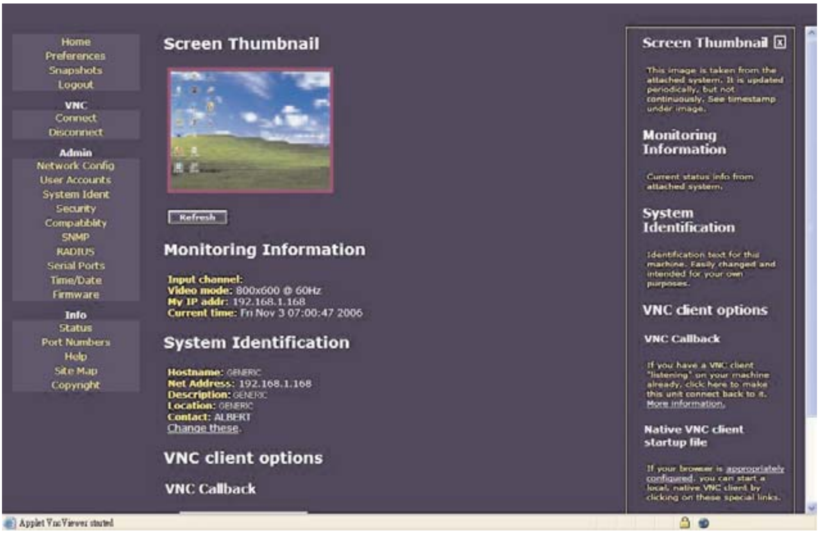
Username admin

Password •••••

Avoid certificate warnings: Download our root public certificate.

Figure 4-1. Login screen.

2. Once you type in the username and password, click on the **Login** button to continue. Figure 4-2 appears.



Screen Thumbnail

Monitoring Information

Input channel:
Video mode: 800x600 @ 60Hz
My IP addr: 192.168.1.168
Current time: Fri Nov 3 07:00:47 2006

System Identification

Hostname: GENERIC
Net Address: 192.168.1.168
Description: GENERIC
Location: GENERIC
Contact: ALBERT
Change these.

VNC client options

VNC Callback

Screen Thumbnail ☒

This image is taken from the attached system. It is updated periodically, but not continuously. See timestamp under image.

Monitoring Information

Current status info from attached system.

System Identification

Identification text for this machine. Easily changed and intended for your own purposes.

VNC client options

VNC Callback

If you have a VNC client "listening" on your machine already, click here to make this unit connect back to it. More information.

Native VNC client startup file

If your browser is appropriately configured, you can start a local, native VNC client by clicking on these special links.

Applet VncViewer started

Figure 4-2. The Home screen.

3. The Home screen (Figure 4-2) serves two functions. First, it is a place to check the ServSwitch unit's status, view essential system information, and capture screen shots from the managed computers. Second, it is where you can start the integrated Java VNC client interaction with the managed computers by clicking on the large screen shot or choosing one of the VNC client links. To refresh the screen, click on the **Refresh** button.

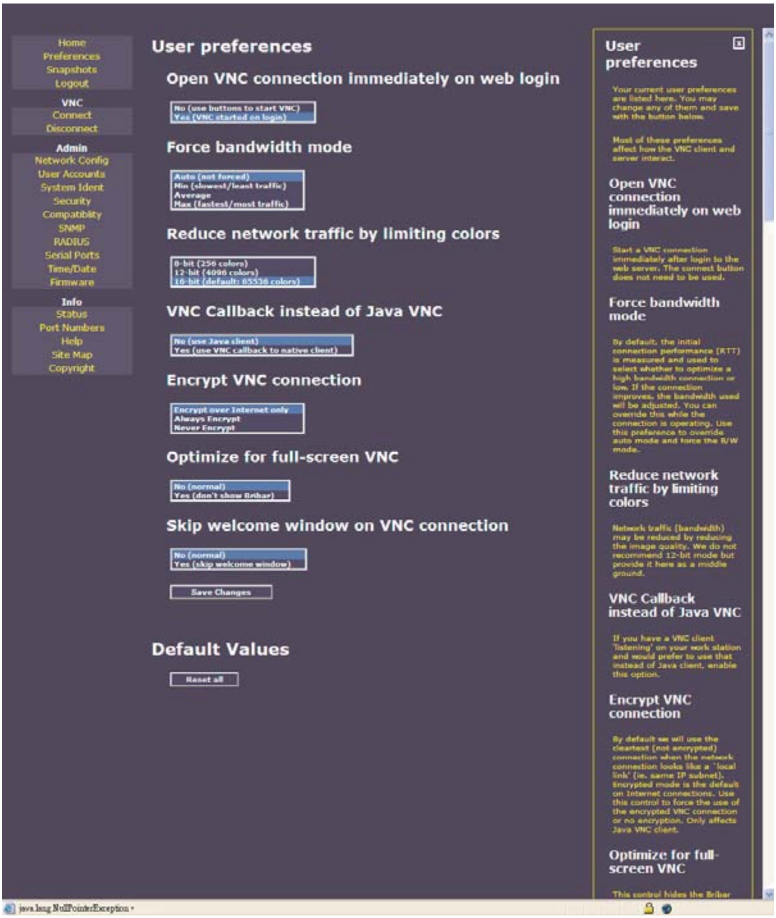
   The menu on the Home screen's left side has 4 categories: Home, VNC, Admin, and Info. Home menu options include Preferences, Snapshots, and Logout. VNC menu options include Connect and Disconnect. Admin menu options include Network Config, User Accounts, System Ident, Security, Compatibility, SNMP, RADIUS, Serial Ports, Time/Date, and Firmware. Info menu options include Status, Port Numbers, Help, Site Map, and Copyright.

   These options are described in **Sections 4.2** through **4.5**.

4.2 Home Menu Options

4.2.1 PREFERENCES

Different user accounts may have different personal preferences. For example, you might have a login account for local access and a different one for remote access. The local account would select 16-bit color, maximum bandwidth, and so on. The remote account would select 8-bit color, low bandwidth, and no splash screen. Plus, the remote account may require encryption. Current user preferences are shown in Figure 4-3.



User preferences

Open VNC connection immediately on web login

No (use buttons to start VNC)
[✓ Yes (VNC started on login)]

Force bandwidth mode

[✓ Auto (not forced)]
Min (slowest/least traffic)
Average
Max (fastest/most traffic)

Reduce network traffic by limiting colors

8-bit (256 colors)
12-bit (4096 colors)
[✓ 16-bit (default: 65536 colors)]

VNC Callback instead of Java VNC

[✓ No (use Java client)]
Yes (use VNC callback to native client)

Encrypt VNC connection

[✓ Encrypt over Internet only]
Always Encrypt
Never Encrypt

Optimize for full-screen VNC

[✓ No (normal)]
Yes (don't show Bribar)

Skip welcome window on VNC connection

[✓ No (normal)]
Yes (skip welcome window)

Default Values

User preferences

Your current user preferences are listed here. You may change any of them and save with the button below.

Most of these preferences affect how the VNC client and server interact.

Open VNC connection immediately on web login

Start a VNC connection immediately after login to the web server. The connect button does not need to be used.

Force bandwidth mode

By default, the initial connection performance (RTT) is measured and used to select whether to optimize a high bandwidth connection or low. If the connection improves, the bandwidth used will be adjusted. You can override this while the connection is operating. Use this preference to override auto mode and force the B/W mode.

Reduce network traffic by limiting colors

Network traffic (bandwidth) may be reduced by reducing the image quality. We do not recommend 12-bit mode but provide it here as a middle ground.

VNC Callback instead of Java VNC

If you have a VNC client 'listening' on your work station and would prefer to use that instead of Java client, enable this option.

Encrypt VNC connection

By default we will use the cleartext (not encrypted) connection when the network connection looks like a 'local link' (ie. same IP subnet). Encrypted mode is the default on Internet connections. Use this control to force the use of the encrypted VNC connection or no encryption. Only affects Java VNC client.

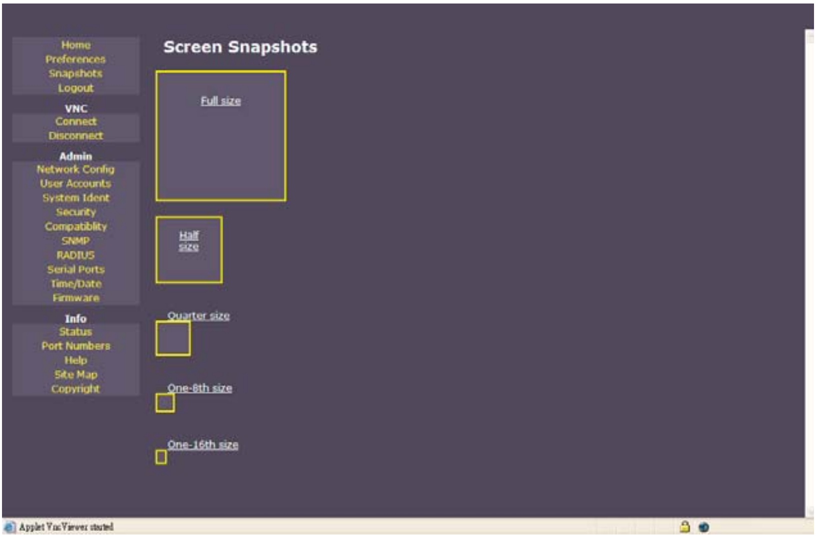
Optimize for full-screen VNC

This control hides the Bribar

Figure 4-3. User Preferences screen.

4.2.2 Snapshots

You can view the screen as full-size, half-size, quarter-size, ⅛th-size, or 1⁄16th-size. Select the appropriate size from the screen shown in Figure 4-4.



Applet VncViewer started

Figure 4-4. The Snapshots screen.

4.2.3 Logout

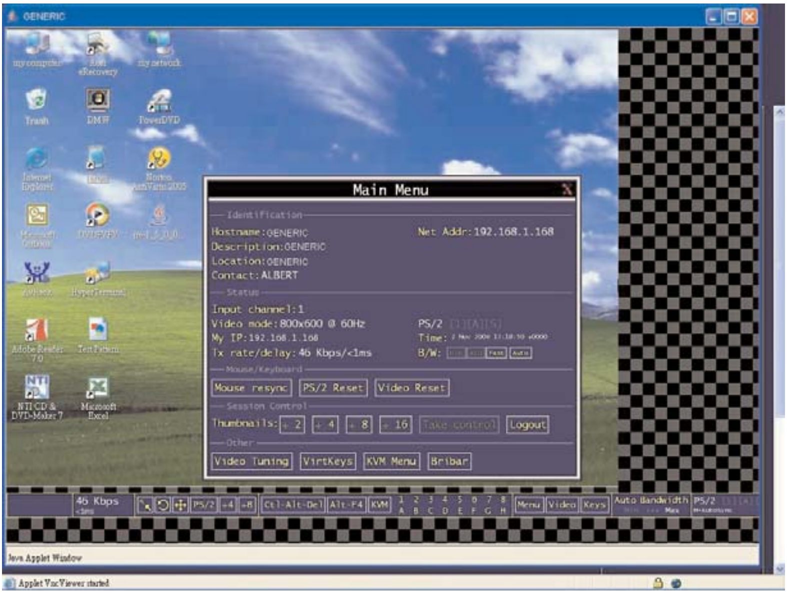
Click on this option to log out.

4.3 VNC Menu Options

You can control the host computers from the VNC menu in the Home screen.

4.3.1 CONNECT

Click on **Connect** from the VNC menu in the Home screen. Figure 4-5 appears. From here, you can control the host computer as if you were physically sitting in front of it.



Main Menu

Identification

Hostname:GENERIC
Description:GENERIC
Location:GENERIC
Contact:ALBERT
Net Addr:192.168.1.168

Status

Input channel:1
Video mode:800x600 @ 60Hz
My IP:192.168.1.168
Tx rate/delay:46 Kbps/<1ms
PS/2

Figure 4-5. The host computer's screen.

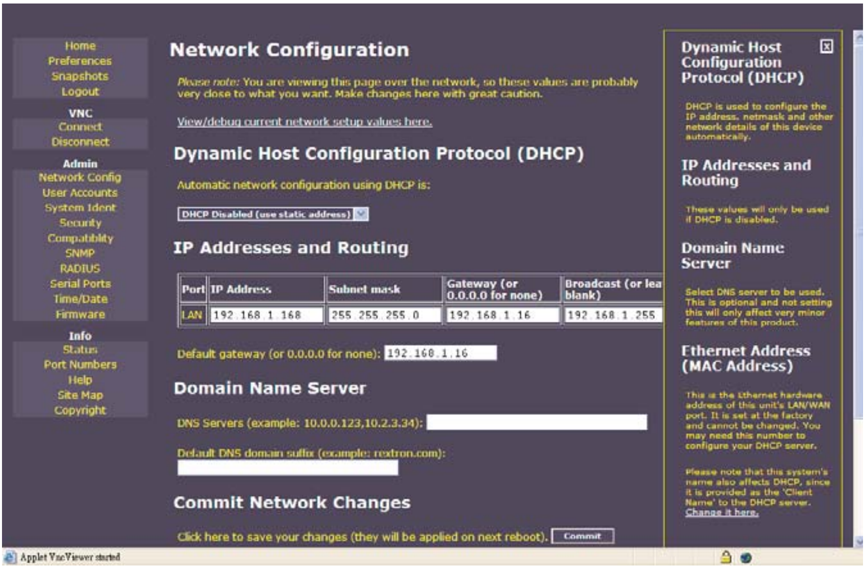
4.3.2 DISCONNECT

To disconnect from the host computer, click on **Disconnect**.

4.4 Admin Menu Options

4.4.1 Network Config

From the Home screen, click on **Network Config**. The screen shown in Figure 4-6 appears.



Network Configuration

Please note: You are viewing this page over the network, so these values are probably very close to what you want. Make changes here with great caution.

View/debug current network setup values here.

Dynamic Host Configuration Protocol (DHCP)

Automatic network configuration using DHCP is:

DHCP Disabled (use static address)

IP Addresses and Routing

Port	IP Address	Subnet mask	Gateway (or 0.0.0.0 for none)	Broadcast (or lea blank)
LAN	192.168.1.168	255.255.255.0	192.168.1.16	192.168.1.255

Default gateway (or 0.0.0.0 for none): 192.168.1.16

Domain Name Server

DNS Servers (example: 10.0.0.123,10.2.3.34):

Default DNS domain suffix (example: rextron.com):

Commit Network Changes

Click here to save your changes (they will be applied on next reboot). Commit

Dynamic Host Configuration Protocol (DHCP)

DHCP is used to configure the IP address, netmask and other network details of this device automatically.

IP Addresses and Routing

These values will only be used if DHCP is disabled.

Domain Name Server

Select DNS server to be used. This is optional and not setting this will only affect very minor features of this product.

Ethernet Address (MAC Address)

This is the Ethernet hardware address of this unit's LAN/WAN port. It is set at the factory and cannot be changed. You may need this number to configure your DHCP server.

Please note that this system's name also affects DHCP, since it is provided as the 'Client Name' to the DHCP server. Change it here.

Figure 4-6. Network Configuration screen.

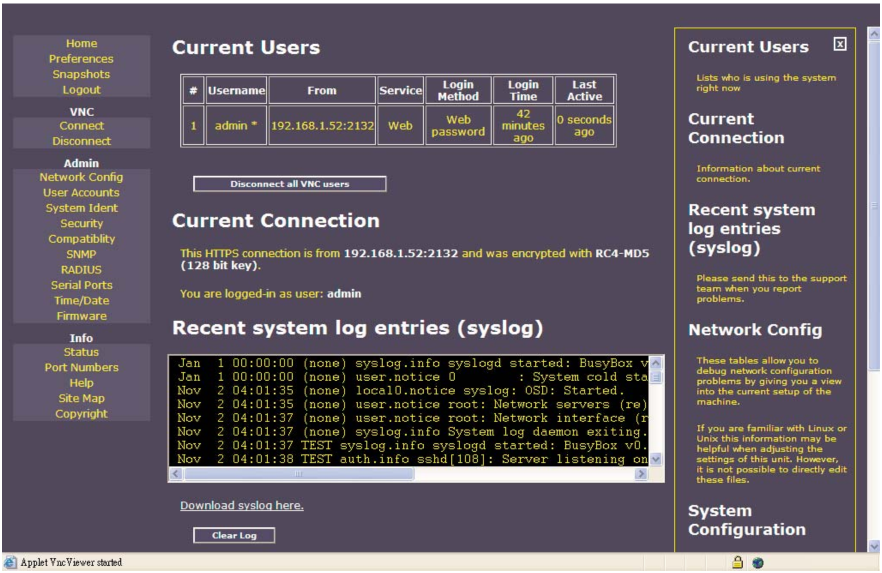
The options shown in Figure 4-6 are described in Table 4-1.

Table 4-1. Network Configuration screen options.

Parameter	Description
Network Configuration	Click on **view/debug current network setup values here**. Figure 4-7 appears (see the next page).
Dynamic Host Configuration Protocol (DHCP)	Select Enabled or Disabled from the drop-down menu. This feature applies to the LAN port on the rear panel and is Enabled by default. When enabled, the unit will automatically configure itself with an IP address when a DHCP server is present. When disabled, the LAN port will use the values assigned to it on the IP Addresses and Routing table at the bottom of Figure 4-6.
IP Addresses and Routing	This table allows you to assign IP information for the LAN port. If you are using DHCP, the values for the LAN port will be filled in automatically and any changes made will not affect the setup. Port: The port is automatically identified as LAN. IP Address: Type in the IP address for the ServSwitch. Subnet Mask: Type in the subnet mask for the ServSwitch. Gateway (or 0.0.0.0 for none): Type in the ServSwitch unit's default gateway. Broadcast (or leave blank): Type in the broadcast address, or leave this field blank.
Domain Name Server	This section allows you to specify DNS servers and the default DNS domain suffix in use on the network. If DHCP is enabled, some of these values may be supplied automatically.
Commit Network Changes	Click on the **Commit** button to apply any changes made on the page to the configuration. The new changes do not take effect until the next time the unit restarts.

View/debug current network setup values here

When you click on this option in the Network Configuration screen (Figure 4-6), the screen shown in Figure 4-7 appears. This screen allows you to monitor the records about current login users, current connection, recent system log entries, and so on.



Current Users

#	Username	From	Service	Login Method	Login Time	Last Active
1	admin *	192.168.1.52:2132	Web	Web password	42 minutes ago	0 seconds ago

Current Connection

This HTTPS connection is from 192.168.1.52:2132 and was encrypted with RC4-MD5 (128 bit key).

You are logged-in as user: admin

Recent system log entries (syslog)

```
Jan  1 00:00:00 (none) syslog.info syslogd started: BusyBox v
Jan  1 00:00:00 (none) user.notice 0          : System cold sta
Nov  2 04:01:35 (none) local0.notice syslog: OSD: Started.
Nov  2 04:01:35 (none) user.notice root: Network servers (re)
Nov  2 04:01:37 (none) user.notice root: Network interface (r
Nov  2 04:01:37 (none) syslog.info System log daemon exiting.
Nov  2 04:01:37 TEST syslog.info syslogd started: BusyBox v0.
Nov  2 04:01:38 TEST auth.info sshd[108]: Server listening on
```

Current Users

Lists who is using the system right now

Current Connection

Information about current connection.

Recent system log entries (syslog)

Please send this to the support team when you report problems.

Network Config

These tables allow you to debug network configuration problems by giving you a view into the current setup of the machine.

If you are familiar with Linux or Unix this information may be helpful when adjusting the settings of this unit. However, it is not possible to directly edit these files.

System Configuration

Figure 4-7. Current Users screen.

Table 4-2. Current Users screen options.

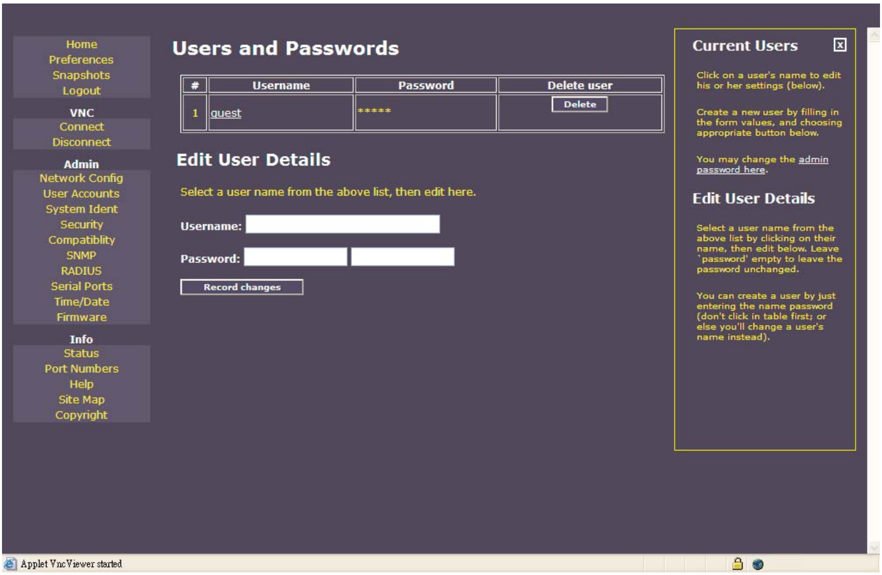
Parameter	Description
Current Users	Create a new user by filling in the form values and choosing the appropriate button below. #: This is the number assigned to the corresponding user. Username: A list of current usernames appears in this field. (Only one username is shown in Figure 4-7.)

Table 4-2 (continued). Current Users screen options.

Parameter	Description
Current Users (continued)	From: The ServSwitch unit's IP address. Service: Indicates a Web connection. Login Method: Indicates a login method. Login Time: The time that the user logged into the system. Last Active: This is the user that was most recently active. Disconnect all VNC users button: Click on this button to disconnect.
Current Connection	Lists the HTTPS IP address connection.
Recent system log entries (syslog)	Lists recent system activity. Download syslog here: Click on this button to download a log entry. Clear Log button: Click on this button to clear all settings.

4.4.2 User Accounts

From the Home screen, click on **User Accounts**. Figure 4-8 appears.



Users and Passwords

#	Username	Password	Delete user
1	guest	*****	Delete

Edit User Details

Select a user name from the above list, then edit here.

Username:

Password:

Current Users

Click on a user's name to edit his or her settings (below).

Create a new user by filling in the form values, and choosing appropriate button below.

You may change the admin password here.

Edit User Details

Select a user name from the above list by clicking on their name, then edit below. Leave `password' empty to leave the password unchanged.

You can create a user by just entering the name password (don't click in table first; or else you'll change a user's name instead).

Figure 4-8. Users and Passwords screen.

This screen allows you to add accounts other than admin to the system. These accounts will not have the authority to change settings, but can access the Web interface and login the VNC console.

Table 4-3. Users and Passwords screen options.

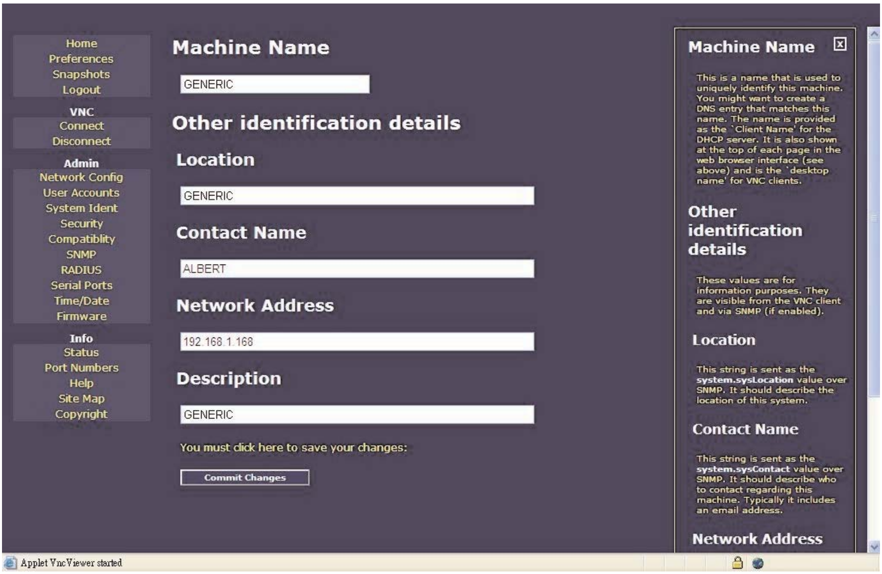
Parameter	Description
Users and Passwords	Create a new user by filling in the form values #, username, and password. #: This is the number assigned to the corresponding user.

Table 4-3 (continued). Users and Passwords screen options.

Parameter	Description
Users and Passwords (continued)	Username: This is the name assigned to the user. Password: The current password is indicated by a row of asterisks. Delete user: Click on the Delete button to permanently remove the displayed user from the system.
Edit User Details	Select a username from the above list (click on its name), then edit the values shown in this form. Leave the password field empty if you do not want to change the password. Username: If you click on a username in the Username field in the Users and Passwords section of the screen, that name will appear in this field. Or, type a new username into this field (or edit an existing username). Password: To keep the password for the selected user the same, leave this field blank. To change the password, type in the new password twice. Record changes button: Click on this button to save your changes.

4.4.3 System Ident

From the Admin menu in the Home screen, click on **System Ident**. The Change System Identification screen (Figure 4-9) appears.



Machine Name

GENERIC

Other identification details

Location

GENERIC

Contact Name

ALBERT

Network Address

192.168.1.168

Description

GENERIC

You must click here to save your changes:

Machine Name

This is a name that is used to uniquely identify this machine. You might want to create a DNS entry that matches this name. The name is provided as the `Client Name' for the DHCP server. It is also shown at the top of each page in the web browser interface (see above) and is the `desktop name' for VNC clients.

Other identification details

These values are for information purposes. They are visible from the VNC client and via SNMP (if enabled).

Location

This string is sent as the **system.sysLocation** value over SNMP. It should describe the location of this system.

Contact Name

This string is sent as the **system.sysContact** value over SNMP. It should describe who to contact regarding this machine. Typically it includes an email address.

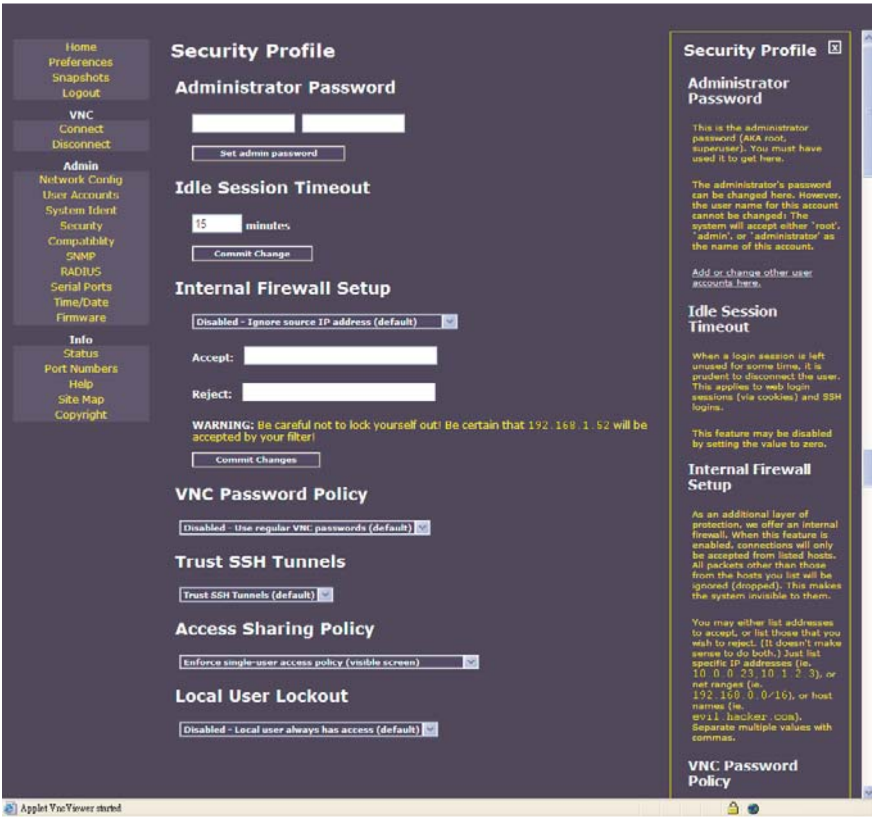
Network Address

Figure 4-9. Change System Identification screen.

The screen options include machine name, location, contact name, network address, and description. These details are useful for DHCP servers, SNMP agents, and VNC clients. Although these values do not affect the ServSwitch unit’s operation, they make it easier to manage PCs or servers on the network. To change any options, type in the changes in the appropriate fields. Then click on **Commit Changes** to save the changes.

4.4.4 Security

From the Home screen, click on **Security.** The Security Profile screen (Figure 4-10) appears.



Security Profile

Administrator Password

Idle Session Timeout

15 minutes

Internal Firewall Setup

Disabled - Ignore source IP address (default)

Accept:

Reject:

WARNING: Be careful not to lock yourself out! Be certain that 192.168.1.52 will be accepted by your filter!

VNC Password Policy

Disabled - Use regular VNC passwords (default)

Trust SSH Tunnels

Trust SSH Tunnels (default)

Access Sharing Policy

Enforce single-user access policy (visible screen)

Local User Lockout

Disabled - Local user always has access (default)

Security Profile

Administrator Password

This is the administrator password (AKA root, superuser). You must have used it to get here.

The administrator's password can be changed here. However, the user name for this account cannot be changed: The system will accept either 'root', 'admin', or 'administrator' as the name of this account.

Add or change other user accounts here.

Idle Session Timeout

When a login session is left unused for some time, it is prudent to disconnect the user. This applies to web login sessions (via cookies) and SSH logins.

This feature may be disabled by setting the value to zero.

Internal Firewall Setup

As an additional layer of protection, we offer an internal firewall. When this feature is enabled, connections will only be accepted from listed hosts. All packets other than those from the hosts you list will be ignored (dropped). This makes the system invisible to them.

You may either list addresses to accept, or list those that you wish to reject. (It doesn't make sense to do both.) Just list specific IP addresses (ie. 10.0.0.23,10.1.2.3), or net ranges (ie. 192.160.0.0/16), or host names (ie. evil.hacker.com). Separate multiple values with commas.

VNC Password Policy

Policy

Figure 4-10. Security Profile screen.

Table 4-4. Security Profile screen options.

Parameter	Description
Administrator Password	The administrator can change the default password for admin (recommended). Read and consider the comments and instructions on this menu before making any changes, as changing these features could make the unit inaccessible through Web configuration (that is, due to firewall filtering). To prevent the chance for error, you must type in the password twice. Set admin password button: Click on this button to save the new password.
Idle Session Timeout	When a login session is left unused for some time, disconnect the user. This applies to Web login sessions (via cookies) and SSH logins. Disable this feature by setting the value to zero. Commit Change button: Click on this option to save the changes.
Internal Firewall Setup	Use this parameter to set up the internal firewall. See the description on the next page. Disabled—Ignore source IP address (default): Select this option from the drop-down menu to disable the IP address. Enabled—Type in a source IP address: Select the IP address to accept or reject. Accept: Type in the desired IP address. Reject: Type in an address you want to disable. Commit Changes button: Click on this button to save the changes.

Table 4-4 (continued). Security Profile screen options.

Parameter	Description
VNC Password Policy	See the description on the next page.
Trust SSH Tunnels	See the description on the next page
Access Sharing Policy	See the description on the next page.
Local User Lockout	See the description on page 41.

The Security menu allows you to configure a number of settings, including:

Internal Firewall Setup

As an additional layer of protection, the ServSwitch can use an internal firewall. When this feature is enabled, connections will only be accepted from listed hosts. For example, the administrator can type in `10.1.0.1/240` in the "Accept" field. The IP of the client's computer between 10.1.0.1 and 10.1.0.240 allows accessing the ServSwitch with the right username and password. On the other hand, the user can type in 192.168.1.0/20 (for example) in the "Reject" field. The IP of the client's computer between 192.168.1.0 and 192.168.1.20 will be rejected to access the ServSwitch. This makes the ServSwitch invisible to them.

There are 3 ways to type in the IP addresses:

1. Specific IP addresses (for example, `10.1.0.1`, `10.1.0.5`, etc.).
2. Net Range (for example, `10.1.0.1/240).`
3. Host Names (for example, `yahoo.com`, `google.com`, etc.).

CAUTION

Be careful NOT to lock yourself out! Be certain that your IP will be accepted by your filter.

VNC Password Policy

When a new VNC connection is established, the remote user must be authenticated. Standard VNC protocol does not support username; it only supports passwords. As long as all users have unique passwords, you can determine which user is connecting based on the password provided. Or, you may enable a second login screen that will require a valid username and password. You must first establish a VNC connection using menus and prompts generated by the firmware.

If it is enabled, a second login screen will be required from Java VNC clients as well. This is unfortunate because the one-time password scheme cannot be used, and Java VNC clients have already logged into the Web server securely. Also, VNC normally encrypts passwords and uses a challenge/hashed response system that is more secure than the second login method. This isn't a concern if the entire connection is encrypted with SSH or SSL, however.

Trust SSH Tunnels

If the incoming VNC connection is coming in over an SSH tunnel, the SSH user/password combination is used and no password is required. Disable this behavior if you suspect that your SSH client machine is not secure and you are concerned that your SSH tunnels may be used by other people.

Access Sharing Policy

There are 3 modes available:

1. Disables—Use regular give/take method (default). By default, all users can take keyboard and mouse control of the system (after connecting via VNC) using a single mouse click.

2. Enforce single-user access policy (visible screen). Some circumstances require more strict control of this capability, so the admin user can select this mode for the highest priority access. With a single-user access policy, only one user may control the host computer(s). New connections are permitted, but they will be able to view the screen *only*, but not control the host computer(s). Once the first user disconnects (or otherwise gives up control), the second user will be able to access the system immediately.

3. Enforce single-user access policy (blank screen contents). Some circumstances require more strict control of this capability. The admin user can select this mode for the highest privacy; no one can see what the admin user is doing from the VNC screen. That is, the admin user can blank the screen contents when another user is connected but not controlling the keyboard and mouse.

With a single-user access policy, only one user may control the system. New connections are permitted, but they will NOT be able to see or even control the host computer(s). Once the first user disconnects (or otherwise gives up control), the second user will be able to access the system immediately. Only the admin user can see or control the host computer(s).

Local User Lockout

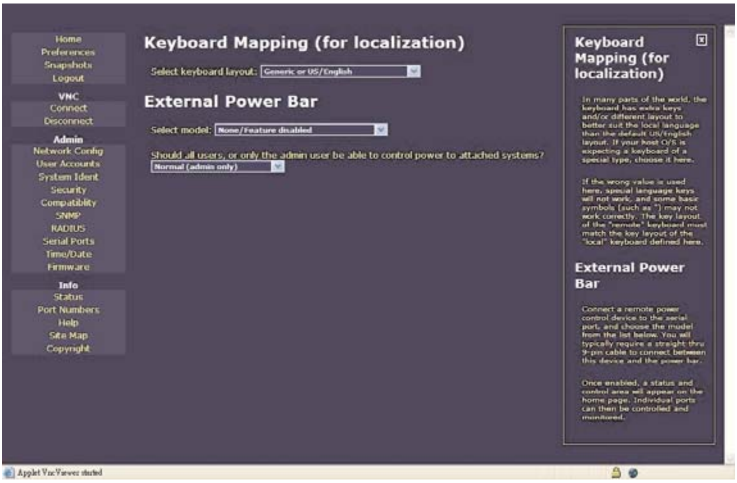
There are 2 modes available:

1. Disabled—Local user always has access (default). Under this mode, the local user has the access right to control the host computer(s).

2. Enabled—Network user given priority. Under this mode, the local user has NO right to control the host computer(s). And on the screen, an IP-OSD menu pops up as the following image shown. The local user can't see or do anything; he can only view the IP-OSD menu shown on the screen. That is, the admin user can select this mode to lock out the local user. Please keep in mind that the local user has no way to take control away from the network user, so an unattended VNC session can cause a problem. Under this situation, if you are locked out of the system because someone has left a VNC session connected and cannot be reached though other means, the admin user may close all VNC connections. See the Status page (see **Section 4.5.1**) to access this feature.

4.4.5 Compatibility

From the Admin menu in the Home screen, click on **Compatibility**. The screen shown in Figure 4-11 appears.



Keyboard Mapping (for localization)

Select keyboard layout: Generic or US/English

External Power Bar

Select model: None/Feature disabled

Should all users, or only the admin user be able to control power to attached systems?
Normal (admin only)

Keyboard Mapping (for localization)

In many parts of the world, the keyboard has extra keys and/or different layout to better suit the local language than the default US/English layout. If your host O/S is expecting a keyboard of a special type, choose it here.

If the wrong value is used here, special language keys will not work, and some basic symbols (such as ") may not work correctly. The key layout of the "remote" keyboard must match the key layout of the "local" keyboard defined here.

External Power Bar

Connect a remote power control device to the serial port, and choose the model from the list below. You will typically require a straight thru 9-pin cable to connect between this device and the power bar.

Once enabled, a status and control area will appear on the home page. Individual ports can then be controlled and monitored.

Applet VncViewer started

Figure 4-11. Compatibility screen.

The options shown in Figure 4-11 are described in Table 4-5.

Table 4-5. Compatibility screen options.

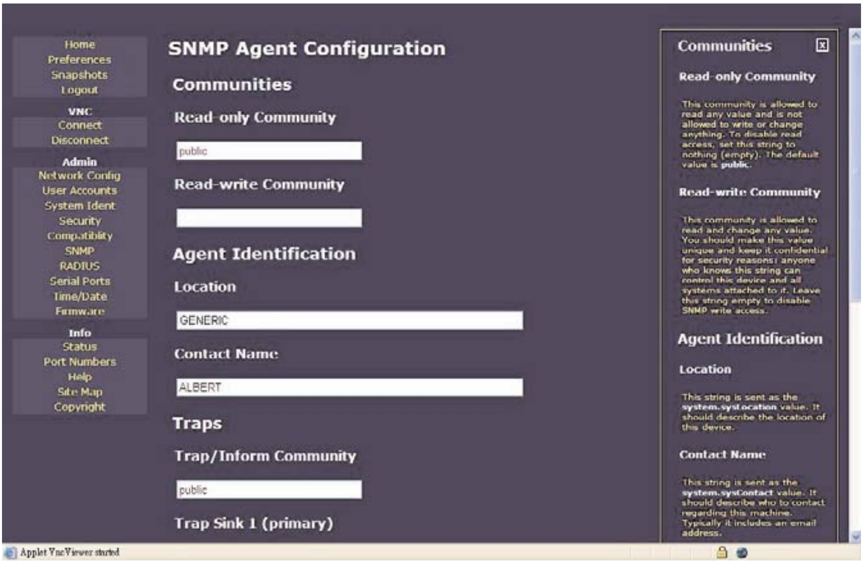
Parameter	Description
Keyboard mapping	In many parts of the world, the keyboard has extra keys and/or a different layout to better suit the local language than the default U.S./English. If your host O/S is expecting a keyboard of a special type, select it from the Select Keyboard Layout drop-down menu. If the wrong value is used here, special language keys will not work, and some basic symbols (such as “) may not even work correctly. The key layout of the remote keyboard must match the key layout of the local keyboard defined here.

Table 4-5 (continued). Compatibility screen options.

Parameter	Description
External power bar	Connect a remote power control device via a straight-through cable to the serial port, and choose the model from the drop-down menu. You *must* use the DB9 serial port (DTE pinout) on the back of the ServSwitch. Once enabled, a status and control window appears. Individual ports can then be power controlled and monitored.

4.4.6 SNMP

From the Admin menu in the Home screen, click on **SNMP**. The menu that appears (Figure 4-12) allows you to configure the ServSwitch so it can be recognized and managed using industry-standard Simple Network Management Protocol (SNMP) software.



SNMP Agent Configuration

Communities

Read-only Community: public

Read-write Community:

Agent Identification

Location: GENERIC

Contact Name: ALBERT

Traps

Trap/Inform Community: public

Trap Sink 1 (primary)

Communities

Read-only Community

This community is allowed to read any value and is not allowed to write or change anything. To disable read access, set this string to nothing (empty). The default value is **public**.

Read-write Community

This community is allowed to read and change any value. You should make this value unique and keep it confidential for security reasons: anyone who knows this string can control this device and all systems attached to it. Leave this string empty to disable SNMP write access.

Agent Identification

Location

This string is sent as the **system.sysLocation** value. It should describe the location of this device.

Contact Name

This string is sent as the **system.sysContact** value. It should describe who to contact regarding this machine. Typically it includes an email address.

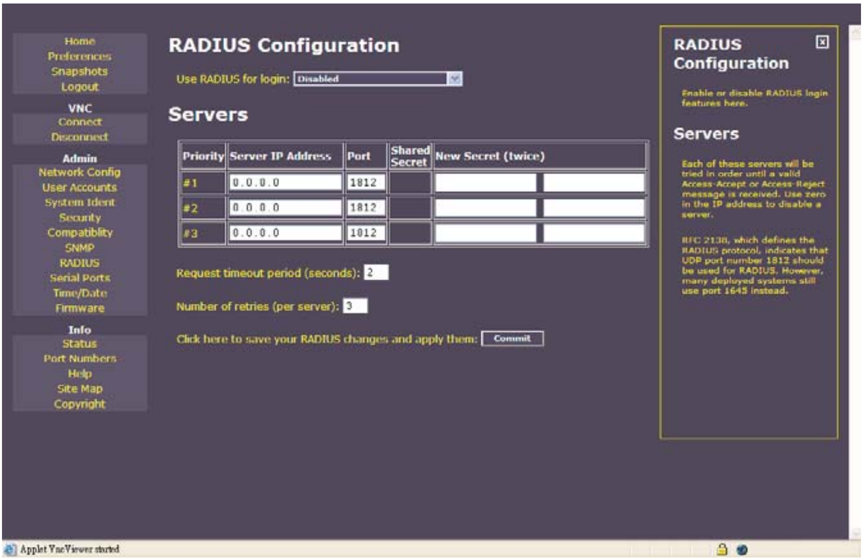
Figure 4-12. SNMP Agent Configuration screen.

Table 4-6. SNMP Agent Configuration screen options.

Parameter	Description
Communities	Set these options to control the ServSwitch. Read-only Community: This community is allowed to read any value and is not allowed to write or change anything. To disable read access, set this string to nothing (empty). The default value is public. Read-write Community: The community is allowed to read and change any value. You should make this value unique and keep it confidential for security reasons. Anyone who knows this string can control this device and all systems attached to it. Leave the string empty to disable SNMP write access.
Agent Identification	This option sets the location and contact name. Location: This string is sent as the system.sysLocation value. It should describe the location of this device. Contact Name: This string is sent as the system.sysContact value. It should describe who to contact regarding this machine. Typically, it includes an email address.
Traps	This option sets the trap settings for the unit. Trap/Inform Community: When trap messages are sent, they are sent using this community. This should be a community that exists on your trap server. Trap Sink 1 (primary): This host will be the target for any traps/inform messages sent. These addresses must be specified numerically. Leave blank if not needed.

4.4.7 RADIUS

From the Admin menu in the Home screen, click on **RADIUS**. The screen shown in Figure 4-13 appears.



RADIUS Configuration

Use RADIUS for login: Disabled

Servers

Priority	Server IP Address	Port	Shared Secret	New Secret (twice)	
#1	0.0.0.0	1812			
#2	0.0.0.0	1812			
#3	0.0.0.0	1812			

Request timeout period (seconds): 2

Number of retries (per server): 3

Click here to save your RADIUS changes and apply them:

RADIUS Configuration

Enable or disable RADIUS login features here.

Servers

Each of these servers will be tried in order until a valid Access-Accept or Access-Reject message is received. Use zero in the IP address to disable a server.

RFC 2138, which defines the RADIUS protocol, indicates that UDP port number 1812 should be used for RADIUS. However, many deployed systems still use port 1645 instead.

Figure 4-13. RADIUS Configuration screen.

The RADIUS server requires the IP address, the UDP port number (1812, default or 1645) and the shared secret. The shared secret is used to encrypt communications and corresponds to a shared password for the RADIUS server and the client machine. Two additional servers may be defined for backup purposes. Each server will be tried in order, using the indicated number of retries and timeout period, which are configurable on the same page. Remember to enable RADIUS after configuring it. While RADIUS authentication is enabled, the locally defined IP module accounts on the ServSwitch will not be used, except for the SSH login. However, if a username of the form “name.local” is given at the RADIUS prompt, the system will use “name”; check the password locally, and skip RADIUS authentication. Delete all local accounts to avoid this behavior. When connecting via VNC, a login screen is generated that asks for a RADIUS username and password.

Table 4-7 describes the options in Figure 4-13.

Table 4-7. RADIUS Configuration screen options.

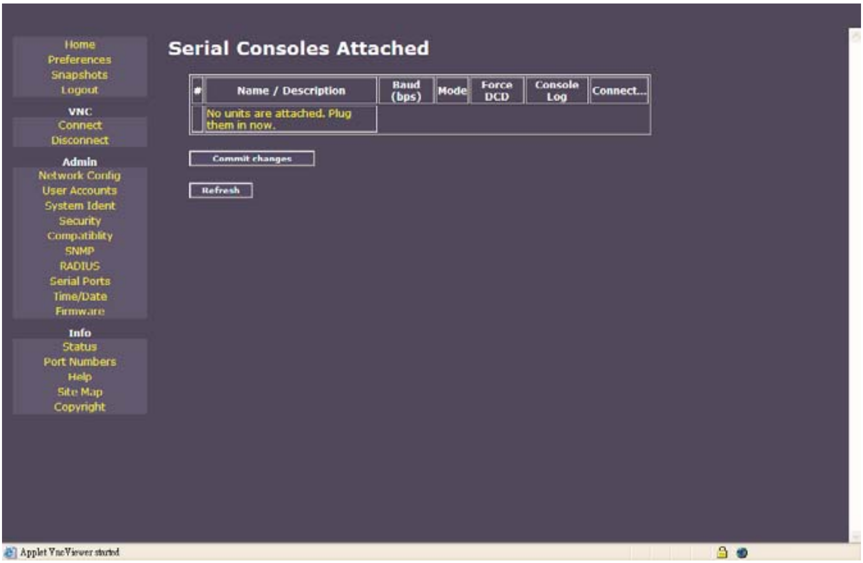
Parameter	Description
Use RADIUS for login	Select Disabled or Enabled from the drop-down menu.
Servers	Priority: Assigns a priority reference number for each server. Server IP Address: Type the IP address into this field. Port: Type in the UDP port number. Shared Secret: This is used to encrypt communications and corresponds to a shared password for the RADIUS server and the client machine. Two additional servers may be defined for backup purposes. Each server will be tried in order, using the indicated number of retries and timeout period, which can be configured on the same page. New Secret: Type in a new value. Type it in a second time.
	Request timeout period (seconds): Type in the timeout period in seconds. This is the amount of time that the ServSwitch will allow to elapse between login retries.
	Number of retries (per server): This is the number of times that the ServSwitch will try to login.

Table 4-7 (continued). RADIUS Configuration screen options.

Parameter	Description
Servers (continued)	Click here to save your RADIUS changes and apply them: Click the **Commit** button to save and apply your changes.

4.4.8 Serial Ports

From the Admin menu in the Home screen, click on **Serial Ports**. Figure 4-14 appears.



Serial Consoles Attached

#	Name / Description	Baud (bps)	Mode	Force DCD	Console Log	Connect...
	No units are attached. Plug them in now.					

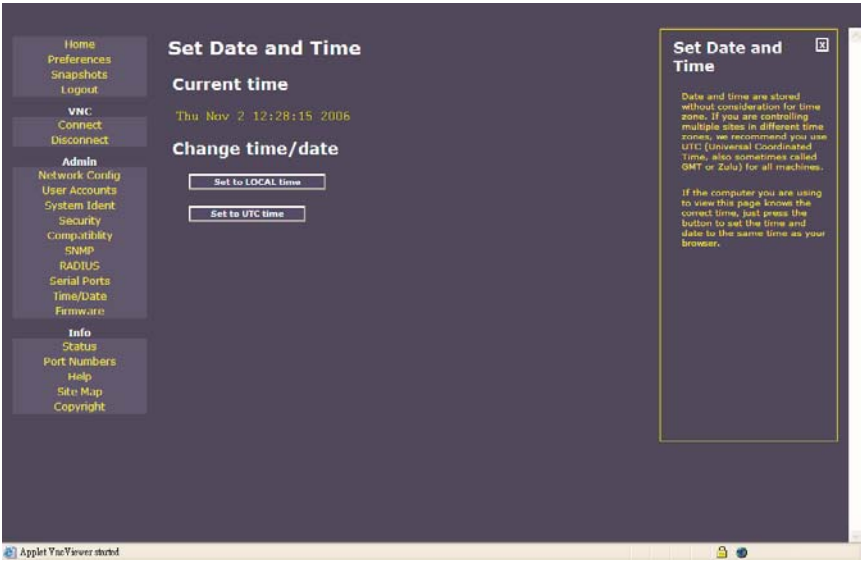
Applet VncViewer started

Figure 4-14. Serial Consoles screen.

There are two ways that the ServSwitch can control the serial devices (power bar, router, printer, and so on). The first way is to connect the serial devices with the ServSwitch unit’s DTE serial port or DCE serial port. The second way is to attach a Serial Access Unit (KV9-SRL) to the ServSwitch unit’s R-port. Once you select the ServSwitch in the Name/Description field in Figure 4-14, click on the **Commit Changes** button to save your selection. To refresh the screen, click on the **Refresh** button.

4.4.9 Time/Date

From the Admin menu in the Home screen, click on **Time/Date**. The screen that appears (Figure 4-15) allows you to set the ServSwitch to Local Time or Universal Coordinated Time (Greenwich Mean Time [GMT]). Date and time from different computers is stored without consideration for time zone. If you are controlling multiple sites in different time zones, we recommend you use GMT for all machines.



Set Date and Time

Current time

Thu Nov 2 12:28:15 2006

Change time/date

Set Date and Time

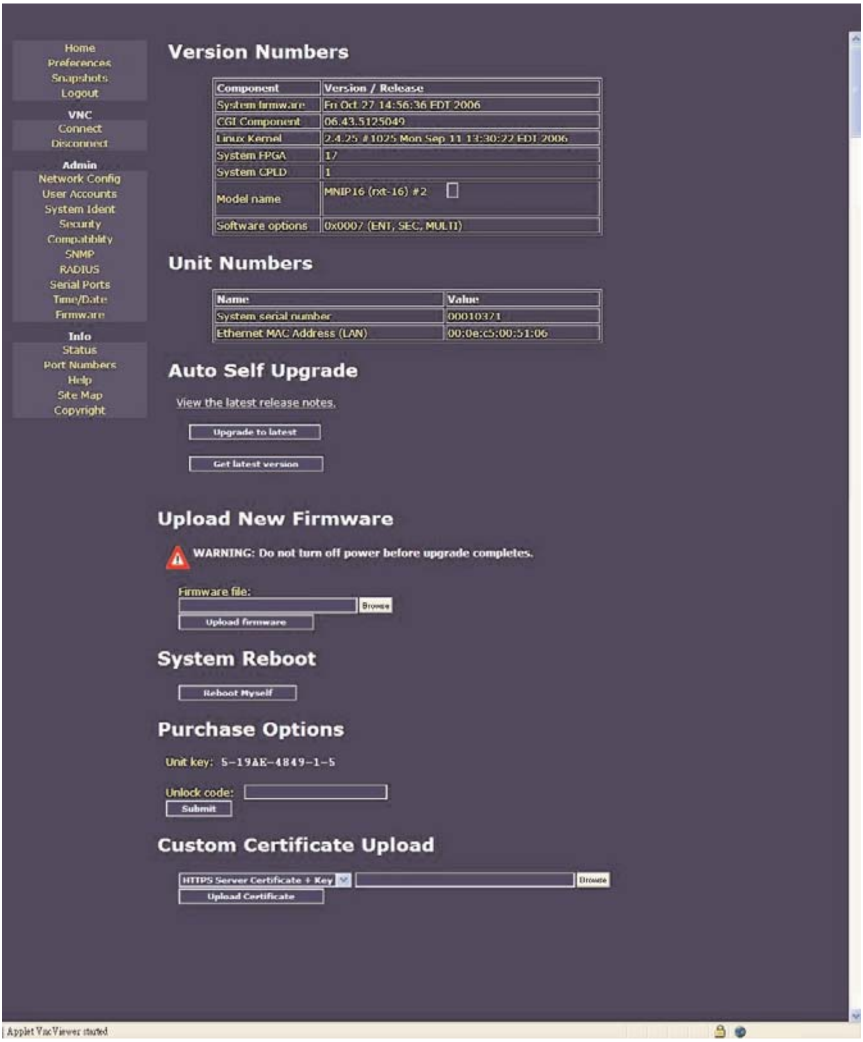
Date and time are stored without consideration for time zone. If you are controlling multiple sites in different time zones, we recommend you use UTC (Universal Coordinated Time, also sometimes called GMT or Zulu) for all machines.

If the computer you are using to view this page knows the correct time, just press the button to set the time and date to the same time as your browser.

Figure 4-15. Set Date and Time screen.

4.4.10 Firmware

From the Admin menu in the Home screen, click on **Firmware**. A firmware upgrade screen (Figure 4-16) appears.



Version Numbers

Component	Version / Release
System firmware	Fri Oct 27 14:56:36 EDT 2006
CGI Component	06.43.5125049
Linux Kernel	2.4.25 #1025 Mon Sep 11 13:30:22 EDT 2006
System FPGA	17
System CPLD	1
Model name	MNIP16 (rxt-16) #2 □
Software options	0x0007 (ENT, SEC, MULTI)

Unit Numbers

Name	Value
System serial number	00010371
Ethernet MAC Address (LAN)	00:0e:c5:00:51:06

Auto Self Upgrade

Upload New Firmware

WARNING: Do not turn off power before upgrade completes.

Firmware file:

System Reboot

Purchase Options

Unit key: 5-19AE-4849-1-5

Unlock code:

Custom Certificate Upload

Applet VncViewer started

Figure 4-16. Firmware upgrade screen.

Table 4-8. Firmware upgrade screen options.

Parameter	Description
Version Numbers	These fields list the firmware version numbers.
Unit Numbers	These fields list the ServSwitch parameters.
Auto Self Upgrade	The ServSwitch includes an innovative feature allowing the unit to upgrade itself over the Internet. Simply click on the button labeled **Upgrade to latest** and the unit will go to the Internet and download the latest version of the system firmware and then install it. If the unit cannot access the Internet directly (perhaps because of a Web proxy or other firewalls), then a page will be shown that causes your browser to download the required file. Save this file to disk and then upload it as described in Manual Upload on page 51. If you have multiple units to upgrade, you may choose the **Get latest version** button that will not attempt to upgrade the unit directly, but will instead fetch the required file. This file can be uploaded to multiple units manually.
Upload New Firmware	Click on the **Upload firmware** button to upload the firmware.
System Reboot	Click on the **Reboot Myself** button to restart the ServSwitch.
Purchase Options	Use this option to customize your software.
Custom Certificate Upload	Select a custom certificate from the drop-down menu, or click on the **Browse** button to view available certificates. Click on the **Upload Certificate** button to upload the selected certificate.

Manual Upload

Enter the name of the firmware file that you just downloaded from the ServSwitch Web site into the field provided in the Firmware upgrade screen (or use the **Browse** button). Press **Upload Firmware** and wait until a successful upload message is shown.

NOTE

Remember the following during the firmware upgrade.

Do NOT turn off power to unit before this operation completes successfully. It may take several minutes to write to flash memory.

The unit will sometimes reboot as part of the upgrade procedure, depending on which system component is upgraded. You will have to reconnect and re-login in those cases.

Wait at least two minutes after pressing Start. Do not assume the upload did not work. There is no status indicator bar to show the progress of the upload. The upload could simply be slow.

Each file that is distributed upgrades a different component of the system. Therefore, be sure to apply all files you are given as part of an upgrade. The system knows what to do with each file you give it, and they are checked for validity before being applied.

How to Upload a Custom Certificate

To upload your own certificate to replace the factory-supplied SSL certificate, scroll down to the bottom of the Firmware upgrade screen (Figure 4-16).

The ServSwitch requires an RSA private key and corresponding public certificate to be combined into one PEM file. There should be no encryption on the private key and it must be first in the file. Therefore, the ServSwitch expects a text file in this format:

—BEGIN RSA PRIVATE KEY—

[based64 encoded key]

—END RSA PRIVATE KEY—

—BEGIN CERTIFICATE—

[based64 encoded certificate]

—END CERTIFICATE—

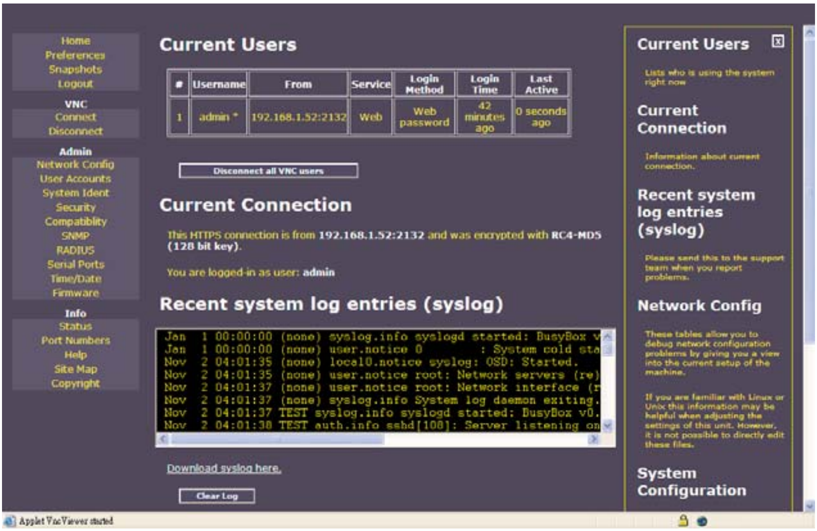
[end of file]

Uploading the root CA public certificate is optional and only affects the link on the login page. It does not affect operation otherwise. It's just an X.509 PEM file holding a public certificate.

4.5 Info Menu Options

4.5.1 Status

From the Info menu on the Home screen, click on **Status** and Figure 4-17 appears.



Current Users

#	Username	From	Service	Login Method	Login Time	Last Active
1	admin *	192.168.1.52:2132	Web	Web password	42 minutes ago	0 seconds ago

Current Connection

This HTTPS connection is from 192.168.1.52:2132 and was encrypted with RC4-MD5 (128 bit key).

You are logged-in as user: admin

Recent system log entries (syslog)

```
Jan  1 00:00:00 (none) syslog.info syslogd started: BusyBox v
Jan  1 00:00:00 (none) user.notice 0         : System cold sta
Nov  2 04:01:35 (none) local0.notice syslog: OSD: Started.
Nov  2 04:01:35 (none) user.notice root: Network servers (re)
Nov  2 04:01:37 (none) user.notice root: Network interface (r
Nov  2 04:01:37 (none) syslog.info System log daemon exiting.
Nov  2 04:01:37 TEST syslog.info syslogd started: BusyBox v0.
Nov  2 04:01:38 TEST auth.info sshd[108]: Server listening on
```

Current Users

Lists who is using the system right now

Current Connection

Information about current connection.

Recent system log entries (syslog)

Please send this to the support team when you report problems.

Network Config

These tables allow you to debug network configuration problems by giving you a view into the current setup of the machine.

If you are familiar with Linux or Unix this information may be helpful when adjusting the settings of this unit. However, it is not possible to directly edit these files.

System Configuration

Figure 4-17. The Status screen.

This menu shows your ServSwitch system status as follows:

- Current Users: Shows the users currently logged in.

- Disconnect all VNC users: In case the users are locked out of the system because someone has left a VNC session connected and cannot be reached through other means, the admin user can close all VNC connections.

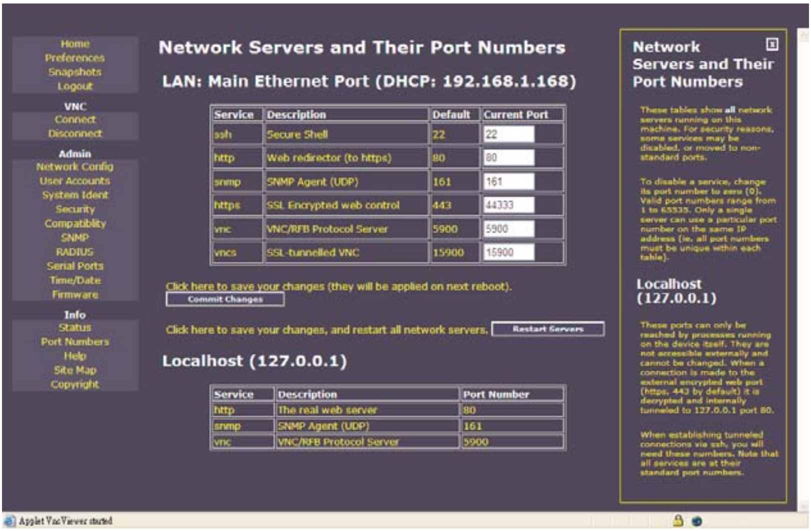
- Current Connection: Shows the current IP and what encryption you are using to log in to the ServSwitch.

- Recent System Log Entries (syslog): Records every log entry, including what time the user logged in, what identification the user logged in, and so forth.

- Network Config: These tables allow you to debug network configuration problems by giving you a view into the current setup of machine. To get to these tables, click on **Network Config** on the right side of the Status screen.
- Click on **Download syslog here** to download the syslog.
- To clear the log, click on the **Clear Log** button.

4.5.2 Port Numbers

From the Info menu on the Home screen, click on **Port Numbers** and Figure 4-18 appears.



Network Servers and Their Port Numbers

LAN: Main Ethernet Port (DHCP: 192.168.1.168)

Service	Description	Default	Current Port
ssh	Secure Shell	22	22
http	Web redirector (to https)	80	80
snmp	SNMP Agent (UDP)	161	161
https	SSL Encrypted web control	443	44333
vnc	VNC/RFB Protocol Server	5900	5900
vncs	SSL-tunnelled VNC	15900	15900

Click here to save your changes (they will be applied on next reboot).

Click here to save your changes, and restart all network servers.

Localhost (127.0.0.1)

Service	Description	Port Number
http	The real web server	80
snmp	SNMP Agent (UDP)	161
vnc	VNC/RFB Protocol Server	5900

Network Servers and Their Port Numbers

These tables show **all** network servers running on this machine. For security reasons, some services may be disabled, or moved to non-standard ports.

To disable a service, change its port number to zero (0). Valid port numbers range from 1 to 65535. Only a single server can use a particular port number on the same IP address (ie. all port numbers must be unique within each table).

Localhost (127.0.0.1)

These ports can only be reached by processes running on the device itself. They are not accessible externally and cannot be changed. When a connection is made to the external encrypted web port (https, 443 by default) it is decrypted and internally tunneled to 127.0.0.1 port 80.

When establishing tunneled connections via ssh, you will need these numbers. Note that all services are at their standard port numbers.

Applet VncViewer started

Figure 4-18. The Port Numbers screen.

The Port Numbers screen shows data about network servers and their port numbers. This data includes LAN: Main Ethernet Port settings and Localhost settings. To apply any changes upon reboot that you make to the LAN: Main Ethernet Port, click on the **Commit Changes** button. To save your changes and restart all servers, click on the **Restart Servers** button.

4.5.3 Help

From the Info menu in the Home screen, click on **Help** to view help screens.

4.5.4 Site Map

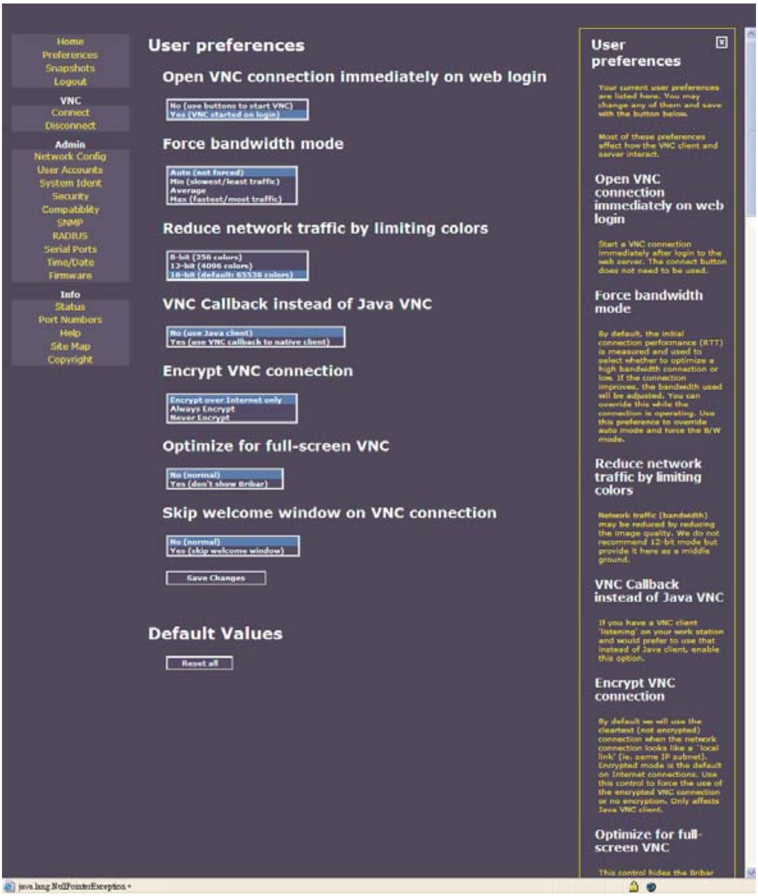
From the Info menu in the Home screen, click on **Site Map** to view information about the site.

4.5.5 Copyright

From the Info menu in the Home screen, click on **Copyright** to view copyright information for the ServSwitch.

4.6 How to Speed Up Your ServSwitch

Click on Preferences on the Home screen and Figure 4-19 appears.



User preferences

Open VNC connection immediately on web login

No (use buttons to start VNC)
Yes (VNC started on login)

Force bandwidth mode

Auto (not forced)
Min (slowest/least traffic)
Average
Max (fastest/most traffic)

Reduce network traffic by limiting colors

8-bit (256 colors)
12-bit (4096 colors)
16-bit (default: 65536 colors)

VNC Callback instead of Java VNC

No (use Java client)
Yes (use VNC callback to native client)

Encrypt VNC connection

Encrypt over Internet only
Always Encrypt
Never Encrypt

Optimize for full-screen VNC

No (normal)
Yes (don't show Bribar)

Skip welcome window on VNC connection

No (normal)
Yes (skip welcome window)

Default Values

User preferences

Your current user preferences are listed here. You may change any of them and save with the button below.

Most of these preferences affect how the VNC client and server interact.

Open VNC connection immediately on web login

Start a VNC connection immediately after login to the web server. The connect button does not need to be used.

Force bandwidth mode

By default, the initial connection performance (RTT) is measured and used to select whether to optimize a high bandwidth connection or low. If the connection improves, the bandwidth used will be adjusted. You can override this while the connection is operating. Use this preference to override auto mode and force the B/W mode.

Reduce network traffic by limiting colors

Network traffic (bandwidth) may be reduced by reducing the image quality. We do not recommend 12-bit mode but provide it here as a middle ground.

VNC Callback instead of Java VNC

If you have a VNC client 'listening' on your work station and would prefer to use that instead of Java client, enable this option.

Encrypt VNC connection

By default we will use the cleartext (not encrypted) connection when the network connection looks like a 'local link' (ie, same IP subnet). Encrypted mode is the default on Internet connections. Use this control to force the use of the encrypted VNC connection or no encryption. Only affects Java VNC client.

Optimize for full-screen VNC

This control hides the Bribar

java.lang.NullPointerException

Figure 4-19. The User Preferences screen.

From this screen, select bandwidth control. There are 4 modes available: Min, Avg, Max, and Auto. If you choose Min, Avg, or Max, you will override the default, Auto. The automatic mode measures actual network performance. You may see the current mode switch from Min to Avg or Max. The different modes indicate more time spent on compression versus more bandwidth. There is no visual difference between the modes, but there can be a noticeable difference in speed and smoothness.

From Force bandwidth mode, you can select the proper bandwidth corresponding to your network environment. We recommend selecting **Max** for LAN users and **Min** for WAN users.

Click on **Open VNC connection immediately on web login** to get the VNC screen (the host computer(s) screen) (Figure 4-20).

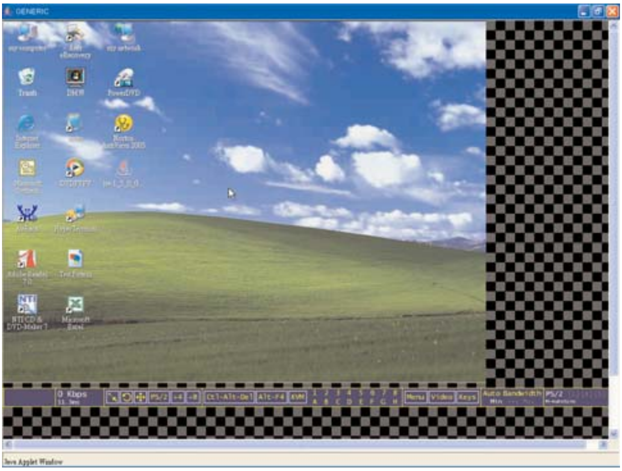


Figure 4-20. The VNC screen.

NOTE

You may need to upgrade or download your Java (*http://www.java.com*) support in your browser before using the VNC screen to remotely control the host computer(s). However, most modern browsers come with a version of Java that's compatible with this application.

5. Accessing ServSwitch Features

Once you access and configure the ServSwitch unit's networking component, you can use it to select and control the managed computers connected to it. This section describes how to add ServSwitch units to the master unit for greater flexibility and how to use the on-screen display (OSD) system to manage your computers. Once you have established a VNC session with the ServSwitch, you can access the KVM features as though you were at a local console.

5.1 Cascade Configuration

You can connect a second level of ServSwitch units to one or more of your ServSwitch units via its PC 1–8 ports. The ServSwitch units connected to the first ServSwitch (the master switch) are known as slaves. Once connected, the units will automatically configure themselves as either masters or slaves. You can only connect an equal or smaller ServSwitch to the master: a 16-port master switch can have both 16-port and 8-port slave ServSwitch units, an 8-port master switch can have 8-port and 4-port slaves, and so on.

For example, the 16-port unit can support 136 computers, with 8 units of 16-port slave ServSwitch units, each connected to 16 computers. The slave ServSwitch units must be connected to the PC 1–8 ports, not the PC A–H ports.

To cascade your ServSwitch units, use a 3-in-1 ServSwitch cable (EHN70001-0006, EHN70001-0010, EHN9000P-0015, or EHN9000P-0030) to connect one of your master switch's PC 1–8 ports to the slave ServSwitch unit's console port. When turning on your cascaded switches, turn on the master switch before turning on any of the others.

Figure 5-1 shows a typical cascade configuration.

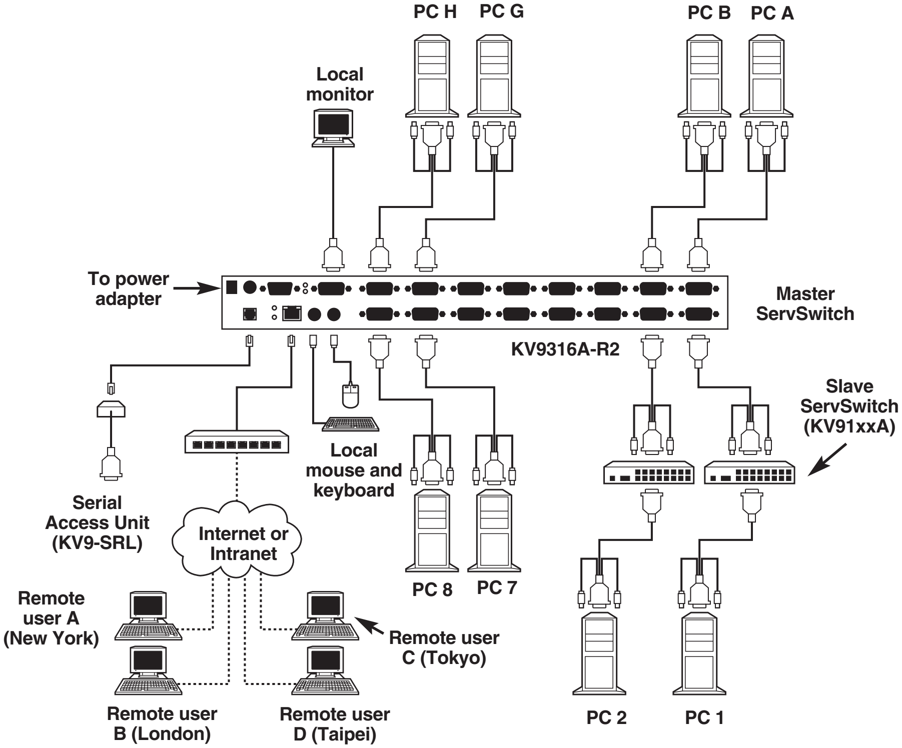
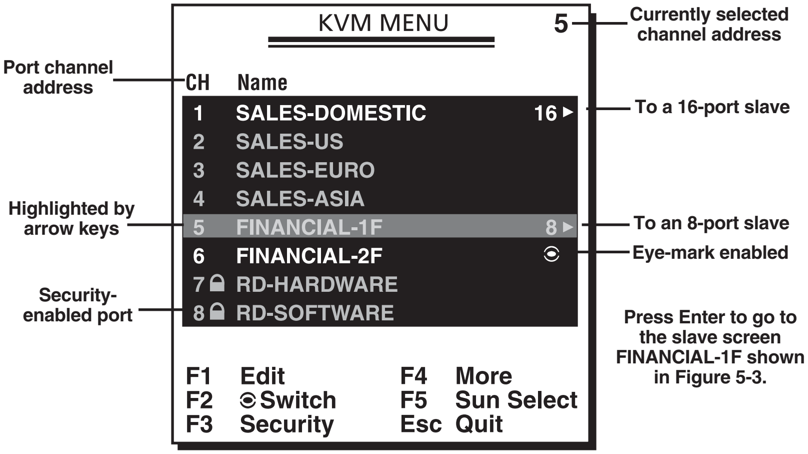


Figure 5-1. Cascade application.

5.2 Selecting Computers Using On-Screen Display (OSD)

The ServSwitch can operate via an on-screen display (OSD). To use this option, press the **Ctrl** key twice within two seconds to see the hotkey menu (an OSD option) if it is enabled. Press the **Left-Ctrl** key three times within two seconds, and a ServSwitch menu screen appears showing a list of the computers with corresponding port numbers, names, and statuses. See Figure 5-2.



KVM MENU 5

CH	Name	
1	SALES-DOMESTIC	16 ▶
2	SALES-US	
3	SALES-EURO	
4	SALES-ASIA	
5	FINANCIAL-1F	8 ▶
6	FINANCIAL-2F	◉
7 🔒	RD-HARDWARE	
8 🔒	RD-SOFTWARE	

Currently selected channel address

Port channel address

To a 16-port slave

Highlighted by arrow keys

To an 8-port slave

Eye-mark enabled

Security-enabled port

Press Enter to go to the slave screen FINANCIAL-1F shown in Figure 5-3.

Figure 5-2. OSD screen.

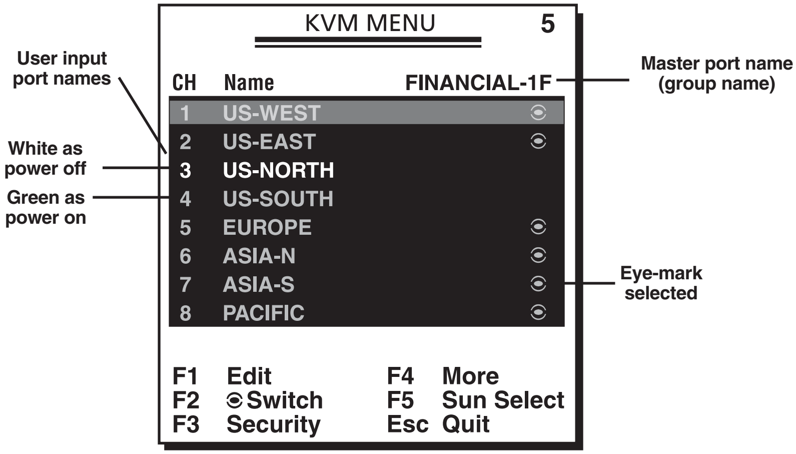
Note also that the short form hotkey menu can be turned on as an OSD function. Just press the F4 key, then select More, then Hotkey menu. See Table 5-1 for hotkey commands.

The port number of the currently selected computer is displayed in red, just like the front indicator, at the upper-right corner of the OSD menu.

In Figure 5-2, the color of a device name is green if it has power and is ready for operation, or the color is white if it has no power. The OSD menu updates the color when the device's power is activated. For 16-port models, press the **PageUp** and **PageDown** keys to view eight other computers.

Press the **up-arrow**, **down-arrow**, **1–8**, or **A–H** keys (depending on the ServSwitch model) to highlight a computer, then press the **Enter** key to select it. Or, press **Esc** to exit OSD and remove the OSD menu from the display. The status window then returns to the display and indicates the currently selected computer or operating status.

A triangle mark to the right of a name (see Figure 5-2) indicates the port is cascaded to a slave; the number at the left of the triangle mark shows the number of ports the slave has. Pressing the **Enter** key brings you one level down and another screen (Figure 5-3) pops up listing the names of the computers on that slave. The name of the slave will be shown at the upper right corner of the OSD menu.



KVM MENU 5

CH	Name	FINANCIAL-1F
1	US-WEST	⦿
2	US-EAST	⦿
3	US-NORTH	
4	US-SOUTH	
5	EUROPE	⦿
6	ASIA-N	⦿
7	ASIA-S	⦿
8	PACIFIC	⦿

F1 Edit F4 More
F2 ⦿Switch F5 Sun Select
F3 Security Esc Quit

Figure 5-3. Slave OSD screen.

An eye mark to the right of a name (see Figure 5-3) indicates that computer is selected and monitored in Scan mode. In the OSD, this mark can be switched on or off by pressing function key **F2**.

Press the **Esc** key to exit OSD and to return to the port/PC screen that you were previously connected to.

The Function and Escape keys work as follows:

Function-key **F1** allows you to edit a computer or slave's name entry with up to 14 characters. First highlight a port, then press **F1** and type the name. Valid characters are A–Z, 0–9, and the dash character. If you type lowercase letters, they will be converted to uppercase ones. Press the **Backspace** key to delete a letter one at a time. Nonvolatile memory stores all name entries until you change them, even if the unit is powered down.

Function-key **F2** allows you to switch a computer's eye mark on or off. First, use the **up-arrow** and **down-arrow** keys to highlight a computer, then press **F2** to switch its eye mark on or off. If Scan Type (described on the next page) is Ready PC, only the power-on and eye-mark selected computers will be displayed sequentially in Scan mode.

Function-key **F3** enables you to lock a computer to prevent unauthorized access. To lock a computer, highlight it and then press **F3**. Now, for the new password, type in up to four characters (A–Z, 0–9) and press the **Enter** key. A security-enabled computer is marked with a lock symbol following its port number. To permanently disable the security function from a locked computer, highlight it, press **F3** and then type in the password.

If you want to access the locked computer temporarily, simply highlight it and press the **Enter** key, then the OSD will ask you for the password. After typing in the correct password, you are allowed to use the computer. This computer is automatically re-locked once you switch to another port. During Scan mode, the OSD skips the password-protected computers.

Function-key **F4** enables more functions, including AutoScan, Manual Scan, Scan Type, Scan Rate, Keyboard Speed, Hotkey Menu, CH Display, Position, Country Code for Sun, and Max. Resolution. A new screen pops up displaying these functions as described on the next two pages. Most of them are marked with a triangle, indicating there are options to choose from. Use the **up-arrow** or **down-arrow** key to select the functions, and then press the **Enter** key. Available options will be shown in the middle of the screen. Again, use the **up-arrow** or **down-arrow** keys to view each option, and then press the **Enter** key to select it.

Function-key **F5** (KV9308A-R2 and KV9316A-R2 only) switches a port's Sun mark on or off to indicate if the computer is a Sun server. Sun servers have more keys on the keyboard than a PC. When you select a Sun marked port, the ServSwitch translates the keys from a PS/2 keyboard to a Sun keyboard. See Keyboard mapping in **Section 4.4.5** for details.

Press the **Esc** key to exit the OSD at any time and return to the port/PC screen that you were previously connected to.

The following functions are what you may choose from when you select the **F4** key.

AutoScan

In this mode, the ServSwitch automatically switches from one powered-on computer to the next one, sequentially in a fixed interval. During AutoScan mode, the OSD displays the name of the selected computer. When AutoScan detects any keyboard or mouse activity, it suspends the scanning until activity stops; it then resumes with the next computer in sequence. To abort the AutoScan mode, press the left **Ctrl** key twice, or press any front-panel button. Scan Type and Scan Rate set the scan pattern. Scan Type (press **F4**, then select More\Scan Type) determines if scanned computers must also be eye-mark selected. Scan Rate (press **F4**, then select More\Scan Rate) sets the duration a computer is displayed before selecting the next one.

Manual Scan

Scan through powered-on computers one by one using the keyboard control. You can press **F4**, then select More\Scan Type to determine if scanned computers must also be eye-mark selected. Press the **up-arrow** key to select the previous computer and the **down-arrow** key to select the next computer. Press any other key to abort the Manual Scan mode.

Scan Type

Ready PC (the powered PC) + eye mark: In Scan mode, scan through powered-on and eye-mark selected computers. Only powered PC and eye-mark selected computers will be scanned.

Ready PC (the powered PC): In Scan mode, scan through powered-on computers. Only powered-on computers will be scanned.

Eye mark only: In Scan mode, scan through any eye-mark selected computer regardless of computer power status. The nonvolatile memory stores the Scan Type setting.

Scan Rate

Sets the duration a computer is displayed in AutoScan mode. The options are 3 seconds, 8 seconds, 15 seconds, and 30 seconds. The nonvolatile memory stores the Scan Rate setting.

Keyboard Speed

The ServSwitch offers a keyboard typematic setting that overrides the similar settings in BIOS and in Windows. Available speed options are Low, Middle, Fast, and Faster at 10, 15, 20, and 30 characters/sec respectively. The nonvolatile memory stores the keyboard speed setting.

Hotkey Menu

When you press the **Left-Ctrl** key twice within two seconds, the Hotkey menu appears, displaying a list of hotkey commands if the option is On. The Hotkey menu can be turned Off if you prefer not to see it when you press the **Left-Ctrl** key twice. The nonvolatile memory stores the Hotkey menu setting.

CH Display

Auto Off: After you select a computer, the port number and name of the computer will appear on the screen for 3 seconds then disappear automatically.

Always On: The port number and name of a selected computer and/or OSD status displayed on the screen continually. The nonvolatile memory stores the CH Display setting.

Position

The actual display position of the selected computer and/or OSD shifts because of different video resolution; the higher the resolution, the higher the display position. Use the **F4** key (More/Position) to select the position of the OSD menu on the screen. Choose from five options: upper-left (UL), upper-right (UR), lower-left (LL), lower-right (LR), or middle (M). The nonvolatile memory stores the position setting.

Country Code for Sun (KV9308A-R2 and KV9316A-R2 only)

Sun keyboards that use different languages have different layouts. The ServSwitch can emulate a Sun keyboard for a specific language or country, such as Arabic, Belgian, U.S., Yugoslavia, and others. Select the proper country code that matches all of your Sun computers.

Max. Resolution

You can adjust the local monitor resolution under this sub-menu. Select 1024 x 768, 1280 x 1024, or 1600 x 1200 for the local monitor. The remote monitor can only have one setting: 1024 x 768.

5.3 Selecting Computers Using Keyboard Hotkey Commands

Each computer is assigned a numeric ID. To directly switch the KVM control to any computer via a simple keyboard command sequence, do the following:

1. To invoke the hotkey mode, press the **Left-Ctrl** key twice within two seconds. The switch will beep to indicate that it's in hotkey mode.
2. Enter your desired switch port number (1–4). For example, if you press **Left-Ctrl Left-Ctrl** 2, you'll select the computer on port 2.

Or, do the following:

1. To invoke the hotkey mode, press the **Left-Ctrl** key twice within two seconds. The switch will beep to indicate that it's in hotkey mode.
2. Press the **up-arrow** or **down-arrow** keys to switch to the previous or next port, respectively.

Table 5-1 lists the hotkey commands.

Table 5-1. Hotkey commands.

Command	Description
<Left-Ctrl><Left-Ctrl> `X`	Switch to PC "X" master port.
<Left-Ctrl><Left-Ctrl> `X C`	Switch PC "X" slave port.
<Left-Ctrl><Left-Ctrl> `F1`	Begin AutoScan. The AutoScan feature allows you to monitor the activity of the connected computers at regular ten-second intervals so that you can monitor the computer activity without having to press the front-panel pushbuttons. This time interval cannot be changed.
<Left-Ctrl><Left-Ctrl>	Stop AutoScan.
<Left-Ctrl><Left-Ctrl> `F2`	Begin Manual Scan.
<Left-Ctrl><Left-Ctrl> <up-arrow>	Switch to previous active PC.
<Left-Ctrl><Left-Ctrl> <down-arrow>	Switch to next active PC.
<Left-Ctrl><Left-Ctrl> `F3`	Adjust scan rate. The ServSwitch beeps one to three times to indicate scan intervals of 3, 8, 15, and 30 seconds.
<Left-Ctrl><Left-Ctrl> `F4`	Adjust keyboard typematic rate (characters per second). The ServSwitch beeps 1 to 4 times to indicate 10, 15, 20, and 30 characters per second. This setting overrides any BIOS or operating system setting.

`X` = 1–8 or A–H; `C` = Slave port number; `F1–F4` = Function keys

Changing Your Configuration

After the initial power on, any device (either a ServSwitch or a PC) can be added or removed from a PC port on the ServSwitch without having to power off the master switch. Make sure that devices are powered off before connecting them to the master switch.

NOTE

After changing your configuration, the OSD will automatically update to reflect the new configuration.

6. How to Remotely Control the Host Computer(s)

6.1 Accessing the VNC Interface

There are three ways to communicate with the ServSwitch in order to control the host computer(s):

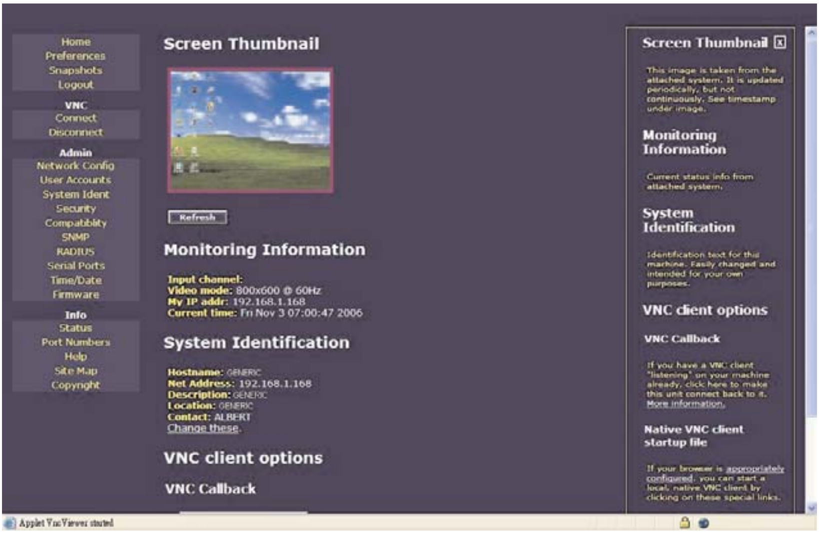
1. Web interface: The integrated Web server includes a Java based VNC client. This allows easy browser-based remote control.

2. Native VNC client: There are several third-party software programs that use the standard VNC protocol, available in open source and commercial VNC clients.

3. SSH Tunnel: By default, there is a standard SSH server running on Port 22 (the standard SSH port). Once connected via SSH, the VNC traffic is tunneled through the SSH connection and encrypts the VNC session. Each method is discussed briefly in the following section. The type of encryption method or client used is not critical.

6.1.1 Web Interface

The Java based VNC client that is integrated into the ServSwitch requires a browser with cookies and JavaScript® enabled. To start the Java VNC client, log in to the Web configuration interface and click on the thumbnail of the desktop on the Home screen, or follow one of the two links on that page. See Figure 6-1.



Screen Thumbnail

Monitoring Information

Input channel:
Video mode: 800x600 @ 60Hz
My IP addr: 192.168.1.168
Current time: Fri Nov 3 07:00:47 2006

System Identification

Hostname: GENERIC
Net Address: 192.168.1.168
Description: GENERIC
Location: GENERIC
Contact: ALBERT
Change these.

VNC client options

VNC Callback

Screen Thumbnail

This image is taken from the attached system. It is updated periodically, but not continuously. See timestamp under image.

Monitoring Information

Current status info from attached system.

System Identification

Identification text for this machine. Easily changed and intended for your own purposes.

VNC client options

VNC Callback

If you have a VNC client "listening" on your machine already, click here to make this unit connect back to it. More information.

Native VNC client startup file

If your browser is appropriately configured, you can start a local, native VNC client by clicking on these special links.

Figure 6-1. The Home screen.

Click on one of the following options (scroll down in the Home screen to see these Java options):

Java VNC with no encryption (faster).

Java VNC with SSL encryption (more secure).

Click on the **Refresh** button to refresh the screen.

NOTE

You may need to upgrade or download your Java (http://www.java.com) support in your browser before using the VNC screen to remotely control the host computer(s). However, most modern browsers come with a version of Java that's compatible with this application.

The Java VNC client makes a connection back to the ServSwitch over Port 5900 (by default) or 15900, if encrypted. The encrypted connection is a standard SSL (Secure Socket Layer) encrypted link that encrypts all data from the session, including the actual video pictures.

Because Java is considered a "safe" programming language, the Java VNC client has some limitations. Certain special keystrokes cannot be sent, such as Scroll Lock on the keyboard.

This client software requires the use of Java 2 (JRE 1.4) to enable features like wheel mouse support. The Sun Microsystems® Java site, *www.java.com*, is an excellent resource to ensure your browser and operating system are up-to-date.

6.1.2 Native VNC Client

This system implements the VNC protocol, so any off-the-shelf VNC client can be used. There are over 17 different VNC clients available and they should all work with this system. This system automatically detects and makes use of certain extensions to the basic RFB protocol that is provided by the better VNC clients.

The best client currently is TightVNC (*www.tightvnc.com*). Binaries are available for Windows, Linux, Mac OS®, and many versions of UNIX. Source code for all clients is available there, too. This version of VNC is being actively developed.

The authoritative version of VNC is available from RealVNC (*www.realvnc.com*). This source base is the original version of VNC, maintained by the original developers of the standard.

For a commercial, supported version of VNC, you should consider TridiaVNC (*www.tridiavnc.com*). Their version of VNC is a superset of TightVNC and contains a number of enhancements for use in a larger corporate environment.

NOTE

Some native VNC clients may require a flag or setting indicating they should use BGR233 encoding by default. If this flag is not set, you may see a garbled picture and the client will fail. The UNIX versions of VNC require the flag -bgr233. For examples on using this flag, see the commands in Section 6.1.3.

6.1.3 SSH Tunnel (with Native VNC Client)

If you are using open SSH, here is the appropriate UNIX command to use, based on the default settings on a machine at 192.168.1.124:

```
ssh -f -l admin -L 15900:127.0.0.1:5900192.168.1.124 sleep 60
vncviewer -bgr233 127.0.0.1::15900
```

NOTES

A copy of these commands, with appropriate values filled in for your current system setting, is provided in the on-line help page. This allows you to cut and paste the required commands accordingly.

You have 60 seconds to type the second command before the SSH connection will be terminated.

NOTES (continued)

The port number 15900 is arbitrary in the above example and can be any number (1025...65535). It is the port number used on your client machine to connect your local SSH instance with the VNC client. If you want to tunnel two or more systems, you will need to use a unique number for each instance on the same SSH client machine.

Some UNIX versions of the VNC client have integrated SSH tunneling support. Some clients require your local user ID to be the same as the user ID on the system.

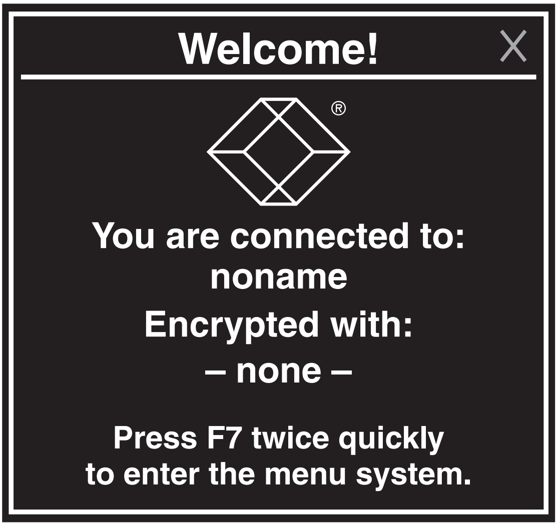
Use a command like this:

```
vncviewer -bgr233 -tunnel192.168.1.124:22
```

6.2 Using the VNC Menu

One of the ServSwitch unit's unique features is the VNC menu system. Whenever you see a window with a dark blue background and gray edges, this window has been inserted into the VNC data stream so that it is effectively laid over the existing video. These menus allow you to control the ServSwitch unit's many features without using the Web interface or a custom client.

To initially connect to the system, double-click on one of the VNC options in the Home screen (Figure 6-1). A window similar to the one shown in Figure 6-2 appears.



Welcome!

You are connected to:
noname

Encrypted with:
– none –

Press F7 twice quickly
to enter the menu system.

Figure 6-2. VNC menu welcome screen.

This tells you which system you are controlling, what encryption algorithm was used, and what key strength is currently in effect. Click anywhere inside the window to clear it or wait ten seconds.

6.3 How to Use the Bribar

Along the bottom of the VNC screen is a dark blue bar with various buttons. We call this feature “the bribar.” Its purpose is to show a number of critical status values and to provide shortcuts to commonly used features.

Figure 6-3 shows a snapshot of what it may look like. There will be slight differences based on optional features and system configuration. Starting from the left side of the bribar, each feature and its function is outlined on the next two pages.

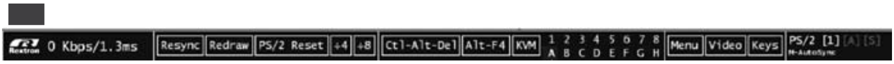
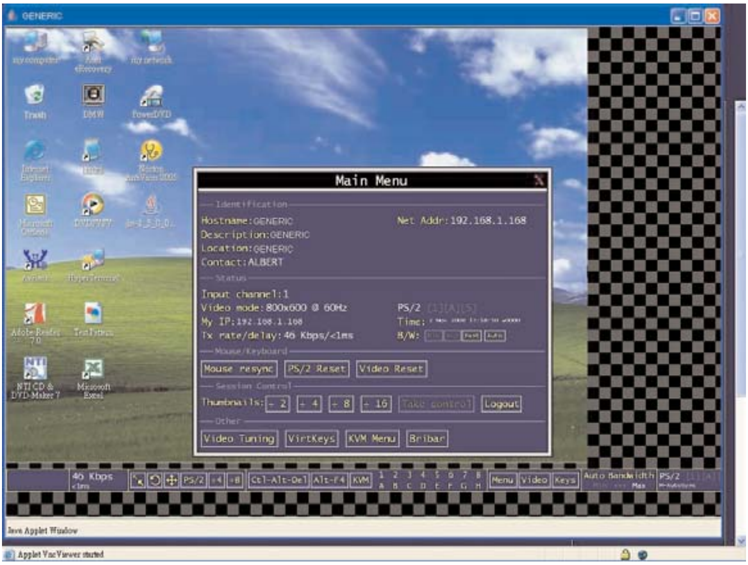


Figure 6-3. A sample bribar.



Main Menu

Identification

Hostname:GENERIC Net Addr:192.168.1.168
Description:GENERIC
Location:GENERIC
Contact:ALBERT

Status

Input channel:1
Video mode:800x600 @ 60Hz PS/2 [1][A][S]
My IP:192.168.1.168 Time:
Tx rate/delay:46 Kbps/<1ms B/W:

Mouse/Keyboard

Mouse resync | PS/2 Reset | Video Reset

Session Control

Thumbnails: ÷ 2 | ÷ 4 | ÷ 8 | ÷ 16 | Take control | Logout

Other

Video Tuning | VirtKeys | KVM Menu | Bribar

Figure 6-4. Main menu.

Bandwidth: Indicates the current average bandwidth coming out of the ServSwitch. The second number measures round trip time (RTT) of the connection when it was first established.

Resync: Re-aligns the remote and local mouse points so they are on top of each other.

Redraw: Redraws the entire screen contents; occurs immediately.

Video Adjust: Adjusts the video phase automatically. (This is an option, even though it doesn't appear in the example shown in Figure 6-3.)

PS/2 Reset: Resets the PS/2 keyboard and mouse emulation. Use this to recover failed mouse and/or keyboard connections in PS/2 mode.

÷4, ÷8: Switches to thumbnail mode, at the indicated size.

Ctrl-Alt-Del: Sends this key sequence to the host. It works immediately.

Alt-F4: Sends the key sequence to host (closes windows).

KVM: Calls up the KVM menu; refer to **Section 5.2** for more information.

1–8, A–H: Select a specific port simply by clicking once on the number or letter.

Menu: Shows the Main menu; refer to **Section 6.4** for more information.

Video: Shows the Video Tuning menu where the picture quality can be adjusted; refer to **Section 6.6** for more information.

Keys: Shows the VirtKeys menu, which allows you to simulate pressing special keys such as the Windows key or complex multi-key sequences; refer to **Section 6.5** for more information.

Auto Bandwidth: Allows you to select the proper bandwidth that corresponds to the network environment. We recommend that you select **Max** for the LAN users and **Min** for the WAN users.

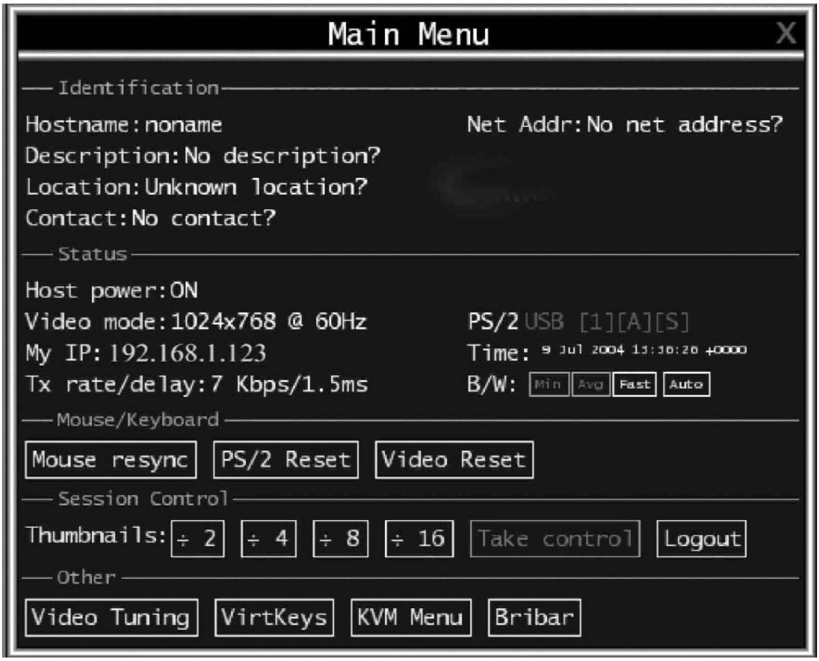
PS/2: This area will show PS/2 (as in this example) to indicate if keyboard and mouse are PS/2 signals. If Autosync appears beneath this indicator, the mouse pointers on the local mouse and the VNC session will be synchronized automatically.

[1][A][S]: These flags show the state of the keyboard lights, NumLock, ShiftLock and ScrollLock respectively.

Other items: If the server's screen resolution is larger than 1024 x 768, additional buttons will be shown to the right of the above listed items. These are all keyboard shortcuts and are duplicated in the Keys menu.

6.4 How to Use the Main Menu

To access the Main menu, press the **F7** key twice within one second, as described in **Section 6.2**. If you press it once or too slowly, then the ServSwitch will not recognize this command. Pressing the **F7** key twice quickly is the only way to get into the menu system if the bribar is disabled. Figure 6-5 shows the Main menu for a typical system.



Main Menu

Identification

Hostname: noname

Net Addr: No net address?

Description: No description?

Location: Unknown location?

Contact: No contact?

Status

Host power: ON

Video mode: 1024x768 @ 60Hz

PS/2 USB [1][A][S]

My IP: 192.168.1.123

Time: 9 Jul 2004 13:30:20 +0000

Tx rate/delay: 7 Kbps/1.5ms

B/W: Min Avg Fast Auto

Figure 6-5. The Main menu.

The Main menu window may be moved by clicking and dragging on the title bar. It can be closed by pressing **Escape** or by clicking on the red X in the top right corner.

Click on the **Bribar** button (located in the Main menu screen's lower right corner) to enable or disable the bribar. Press the **F7** key twice to start the Main menu, then click on the bribar to restore the feature.

Various fields from the Main menu are outlined in the text below and on the next page. Most of the functions operate immediately. Other functions require a response to a confirmation prompt first before performing the requested function.

Identification

Fixed text label that is defined by the user in the Web interface. This does not affect the operation of the system and is intended to assist with administration.

Status

Current status of the attached system and the status of the module.

B/W: Min/Avg/Max/Auto (bandwidth control)

The white button is the mode in which the system is currently operating. If you choose Min, Avg, or Max then you will override the default, Auto. Because the automatic mode measures actual network performance, you may see the current mode switch from Min to Avg or Max. The different modes indicate more time spent on compression versus more bandwidth. There is no visual difference between the modes, but there can be a noticeable difference in speed and smoothness.

Mouse Resync button

Click on this button to resynchronize the mouse pointer so that the local and remote mouse pointers are on top of each other.

PS/2 Reset button

Click on this button to reset the PS/2 emulation going to the host and to the attached PS/2 devices. This can be used if the mouse stops responding or the PS/2 keyboard isn't working.

Video Reset button

Click on this button to reset the input video. When you click on this button, the entire VNC screen refreshes.

Thumbnails

Switch to smaller thumbnail size screen images (click anywhere on thumbnail to restore it). Each button corresponds to a different sized image, from half size to one-sixteenth.

Take Control button

When multiple users are connected to the same system, click on this button to take control away from another user. Only one user may control the keyboard and mouse at any time. All users see the same picture.

Logout button

Click on this button to end the VNC session and disconnect.

Video Tuning

Click on this button to access a submenu with video adjustments, if automatic picture adjustment does not provide a good quality picture (see **Section 6.6**).

VirtKeys button

Click on this button to access the virtual keyboard. Virtual keyboard provides a menu with special keys that are often hard to generate but needed by the remote system. The most common key sequence is the Ctrl–Alt–Del (see **Section 6.5**).

KVM Menu button

Click on this button to generate the key sequence used to access the onscreen menu for an enterprise-class ServSwitch or other KVM switch. When these conventional KVM switches are combined with the ServSwitch units described in this manual, this key makes accessing their built-in menu easier, especially from the Java client. This button will only be shown when an external KVM has been enabled via the Web interface.

Bribar button

Click on this button to close or reopen the bribar window at the bottom of the screen.

6.5 How to Use the VirtKeys Menu

Figure 6-6 shows the Virtual Keys window. To get to this screen, click on the VirtKeys button in Figure 6-5.

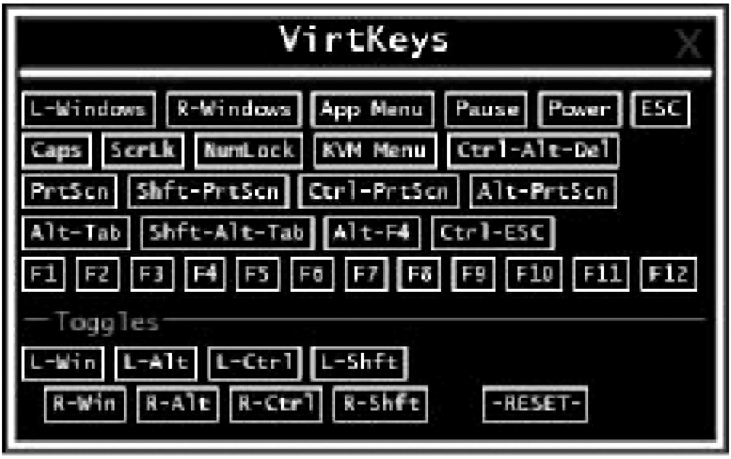


Figure 6-6. VirtKeys screen.

Clicking any button in the top half of the window simulates pressing and releasing the indicated key. In the bottom area of the screen, the Toggles section, clicking will also simulate the indicated key being pressed. You may then click in the top part to send another key and release the key at the same time. Alternatively, you may move the mouse outside this window, press the regular key, and then click on the **Reset** button to release all depressed keys.

The VirtKeys menu can be left open while using the host system. You can then click the required button at the suitable time and still interact with the host in a normal fashion.

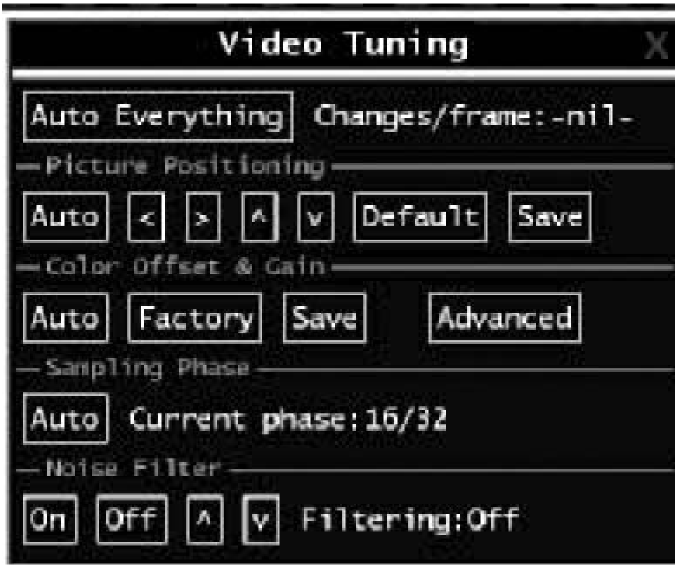
Examples:

<Ctrl> <Alt> <F4> : Use L- Ctrl then L- Alt in the Toggles area. Then click on **F4**.

To bring up the Start menu under Windows: Click the L-Windows button at the top left of the above window.

6.6 How to Use the Video Tuning Menu

This menu (Figure 6-7) is used to fine-tune the video picture. To get to this screen, click on the **Video Tuning** button in Figure 6-5.



Changes/frame:-nil-

Current phase:16/32

Filtering:Off

Figure 6-7. Video Tuning menu.

The text on the next two pages describes the Video Tuning menu options.

Auto Everything

Press this button to automatically fine-tune all three adjustments. If the test pattern for Color Offset calibration is not present on the screen, then the Color Offset adjustment is skipped.

Changes/frame

Press this button to indicate the number of 16 x 16 blocks of video that are being sent, on average, for every frame of video. With a static image being displayed by the server, this number will be zero (shown as -nil-). Moving the mouse, for example, will cause the number to jump to about 2 or 3. You may use this number to judge the picture quality as you adjust the controls on this menu.

Picture Positioning

This option affects the image position on your screen. If you see a black line on either side of your screen, or at the top or bottom, you can use the arrow buttons to shift the image in that direction. Pressing **Auto** does the same thing for you automatically. Use **Save to** save the changes you have made manually. Since this adjustment depends on the video mode, separate values are stored for each video mode.

Color Offset & Gain

This is a fine-tuning adjustment that requires the use of a test pattern. There is a copy of the test pattern available on the Help menu of the integrated Web server. Download that image to the host computer(s). Do not allow scaling, cropping or any other changes to that image. Press the **Auto** button and the system will calibrate color for the best possible picture in approximately one minute. If the system cannot find the test pattern on the screen, it will say so. Check that the pattern isn't scaled or covered up. It's important to do this operation in 24-bit or 32-bit color video mode (that is, true color). Although the algorithm may work in 16-bit or 8-bit color video modes, the results will not be optimum and usually it won't be able to recognize the test pattern.

Advanced

Press this button to open the Advanced Video Tuning menu. While the vast majority of users will not need to adjust these settings, it offers a high degree of control of the video settings of your VNC sessions.

Sampling Phase

This option does not normally need to be used since the ServSwitch tunes the sampling phase whenever the video mode changes. This button does not require a test pattern, but will perform optimally when used with the ServSwitch unit's standard test pattern. For your reference, the sampling phase number is shown to the right of the Filtering button.

Noise Filter

This controls the ServSwitch unit's advanced video filtering feature. Unlike other filtering algorithms, the ServSwitch unit's noise filter will only remove noise. It does not degrade the signal quality or readability of small text. You may turn it on and off using the indicated button, or set it to other values using the arrows. Higher numbers cause more filtering and may cause artifacts when moving windows. The most common visual artifact is a vertical line dropping when moving windows horizontally. You may use the Redraw button to correct these or use a lower filter number. This value must be greater than two.

Appendix A. Troubleshooting

A.1 Problems/Solutions

NOTE

If you are experiencing trouble with your devices, first make sure that all cables are connected to their proper ports and are firmly seated.

Problem: How do I bring up the IP-OSD menu?

Solution: Using a paper clip or pen, press the IP Setup button once to bring up the IP-OSD menu.

Problem: How do I reset everything back to the factory-default values?

Solution: Using paper clip or pen, press the Reset button and hold for about 8 seconds. The IP-OSD menu will automatically appear and show **All settings cleared** in red text, and all of the factory-default values will be restored automatically.

Problem: I can't connect to the ServSwitch.

Solution: Make sure the network connection is working (PING the ServSwitch unit's IP address). If not, check the network hardware. Is the ServSwitch powered on? Make sure the ServSwitch unit's IP address and all other IP-related settings are correct. Also verify that all the IP infrastructure of your LAN, such as routers, are correctly configured. Without a PING functioning, the ServSwitch can't work.

Problem: I can't log in via SSH.

Solution: Was the correct username and password given? The default username and password as shipped from the factory is username `admin` with a password of `admin`. Configure your browser to accept cookies. The username and password are case sensitive, so check the status of the Caps Lock key on your keyboard. If you see a warning such as "identity of host cannot be verified," and a question about saving the host's fingerprint, this is normal for the first time you connect to any machine running SSH. You should answer "yes" so that your SSH client saves the host's public key and doesn't re-issue this warning.

Problem: I forgot the master password.

Solution: Reset the master password. Refer to **Section 4.4.4**.

Problem: The mouse on the remote site does not work or is not synchronized.

Solution:

1. Make sure there is only one mouse driver installed in each computer.
2. Set the mouse acceleration to **None** in the host mouse driver properties.
3. Windows XP has a setting called **Enhance pointer precision**. Disable this setting for correct mouse synchronization.

Problem: The remote mouse and the local mouse don't line up.

Solution: Use the "mouse resync" command in the Main menu or press the **Resync** button on the bribar. If the mouse pointers still don't line up, verify that mouse acceleration has been disabled.

NOTE

The Windows login screen does not accept the mouse acceleration option and always has the mouse accelerated regardless of your configuration. Therefore, on this screen it is best to avoid using the mouse.

Problem: After Resync, the mouse on the remote site is synchronized, but there is small constant offset between remote and local mouse cursors.

Solution: This is a video-position error. Normally, a slight video-positioning error is perceived as a mouse sync issue. A video-positioning error is visible as a black line along the top or bottom (and right or left) edges of the remote screen. On the Video Tuning menu (refer to **Section 6.6**), use the arrows under Picture Positioning to move the screen until the two pointers line up exactly. Remember to save your position changes.

Problem: The monitor works, but the keyboard and mouse do not.

Solution: Make sure you haven't swapped the keyboard and mouse cables.

Problem: The VGA image is not clear.

Solution: You may be using poor-quality VGA cables. Make sure you are using UL® 2919 rated, double-shielded VGA cables.

Problem: The quality of video is bad or the picture is grainy.

Solution:

1. Use the brightness and contrast settings.
2. Use the auto-adjustment feature to correct a flickering video.
3. Read and use **Section 6.6**.
4. Also, try the **Auto Everything** button on the Video Tuning menu.
5. Display the test pattern on the host.
6. Try a lower refresh rate (60 Hz is best).
7. Enable the noise filter and set it to a higher value.
8. Use lower resolution, if possible (1024 x 768).
9. Reduce the number of colors (8-bit or 16-bit color instead of 24/32).
10. Use a better-quality video card.

Problem: No OSD screen or screen image appears.

Solution: You may have selected a powered-off computer. Use the pushbuttons to select a computer that is powered on.

Problem: There is a keyboard error on boot.

Solution: You may have a loose keyboard connection. Make sure your keyboard cables are well seated.

Problem: The letters on the TFT LCD display are blurry or have shadows.

Solution: You may have improper resolution settings. Under the Control Panel, set the VGA output of your computers to match the highest resolution of the LCD monitor with **Large Font** selected.

Problem: The master/slave does not work or there is a double OSD.

Solution:

1. Make sure that the slave's console port is connected to one of the master's PC ports.
2. Perform a KVM reset. Make sure that you have removed all power sources from the slave unit before connecting it to the master switch.

Problem: The OSD menu is not in the proper position.

Solution: The OSD menu has a fixed resolution, and its size varies depending on the monitor. Use **F4**, More/Position (from the OSD menu) to move the OSD menu to a different location.

Problem: The up- and down-arrows don't work in Manual Scan mode.

Solution: Make sure more than one computer is turned on. Manual Scan only works with powered computers. Check the scan type (from the OSD menu) and make sure you have selected the proper computers.

Problem: AutoScan does not work.

Solution: Make sure more than one computer is turned on. AutoScan only works with powered-on computers. Check the scan type (from the OSD menu) and make sure you have selected the proper computers. Press the **Left-Control** key twice or press any front pushbutton to abort the AutoScan.

Problem: I cannot select a computer connected to a slave.

Solution: Make sure that the slave's console port is connected to one of the master's PC ports. Only Ports PC 1 to PC 8 can be connected to slaves, even if the master switch has 16 PC ports.

Problem: Keyboard strokes are shifted.

Solution: Press both **Shift** keys.

Problem: A certificate warning is shown while connecting via HTTPS.

Solution: It is normal for a warning dialog to be shown when connecting via HTTPS. The SSL certificate the ServSwitch uses is created when the unit is first produced. It does not contain the correct hostname (subject name) because you can change the hostname as required. For more details, refer to **Appendix C**.

Problem: Windows XP doesn't awake from standby mode.

Solution: This is possibly a Windows XP problem. Try not to move the mouse while XP goes into standby mode.

Problem: The terminal connection to the ServSwitch for initial configuration cannot be established.

Solution: Check that the null-modem cable connected to DCE serial port on the ServSwitch and terminal software is set to the following line parameters:

Connection speed: 115200 bps
No. of bits: 8
Parity: None
Stop bits: 1
Flow Control: None

Connect a computer to the ServSwitch and power this computer on. Power on the ServSwitch while pressing the **ESC** key on the keyboard connected to it. This will switch the DCE Serial Port 1 to configuration login setting even if it was set to pass-through or modem.

Also, Windows HyperTerminal has a bug: if you change baud rates while connected, the screen is updated but the hardware is still at old baud rate. Hang up and reconnect (using the icons at the top of the screen) to make new settings take effect.

Problem: If my network has a firewall, what setting do I use on the ServSwitch to open a port into the network?

Solution: You shouldn't change any settings in the ServSwitch, but you should open Port 22 for both outbound and inbound connections in your firewall.

Port 22 only needs to be opened for inbound connections. You must use the SSH tunnel to connect to the machine; tunnel to port 127.0.0.1:5900 for VNC protocol, and 127.0.0.1:80 for HTTP (Web) control.

Or, instead of the SSH client, open Ports 443 and 15900 (inbound) for HTTPS and encrypted VNC protocol. Then click on the "encrypted" link. This is easier because you don't need to set up SSH tunnels.

A.2 Calling Black Box

If you determine that your 4-, 8-, or 16-Port ServSwitch EC Series IP KVM Switch is malfunctioning, do not attempt to alter or repair the unit. It contains no user-serviceable parts. Contact Black Box at 724-746-5500.

Before you do, make a record of the history of the problem. We will be able to provide more efficient and accurate assistance if you have a complete description, including:

- the nature and duration of the problem.
- when the problem occurs.
- the components involved in the problem.
- any particular application that, when used, appears to create the problem or make it worse.

A.3 Shipping and Packaging

If you need to transport or ship your 4-, 8-, or 16-Port ServSwitch EC Series IP KVM Switch:

- Package it carefully. We recommend that you use the original container.
- If you are shipping the 4-, 8-, or 16-Port ServSwitch EC Series IP KVM Switch for repair, make sure you include everything that came in the original package. Before you ship, contact Black Box to get a Return Authorization (RA) number.

Appendix B. Supported Protocols

Service	Description	Benefits
SSH	Secure Shell	May be used to securely tunnel VNC and HTTP protocols.
HTTP	Web redirector (to HTTPS)	Convenience server to redirect all Web traffic to an encrypted port. Clear-text HTTP is not supported.
SNMP	SNMP Agent (UDP)	Allows integration with existing SNMP network management systems.
HTTPS	SSLTLS Encrypted Web control	Secure control and management of the device and attached system. Screen snapshots may be downloaded. Integrated Java VNC client (with or without encryption) allows control from any Java enabled browser. Password protected.
VNC	VNC/RFB Protocol Server	Standardized real-time KVM network protocol. Compatible with existing VNC client software.
VNCS	SSL-tunneled VNC	VNC protocol tunneled via SSL TLS encryption. Used for secure real-time server control over public networks.
DHCP	Dynamic IP Setup Config	Eases network setup by fetching IP address and other network settings from a centralized server.

Service	Description	Benefits
RADIUS	Centralized authentication	Allows integration with existing RADIUS servers, so that user management can be centralized. Supports challenge-response authentication using hardware tokens (like SecurID) and conventional passwords.
SYSLOG	System event logging to another system	MIT-LCS UDP protocol. Must be configured via DHCP option.
DNS	Domain Name Service	Converts text name into IP address only used in the URL specification needed to emulate a CD-ROM. Using this is optional.

Appendix C. About Security Certificate Warnings

C.1 Frequently Asked Questions

What is a security certificate?

Sites that employ secure TCP/IP (Internet) connections include a certificate that confirms that users are connecting to a legitimate site and are not being redirected without their knowledge. Certificates are issued by trusted third parties called Certificate Authorities (CAs) and contain essential details about a site that must match the information supplied to your Web browser.

Why do I receive a warning when I access the login screen on the ServSwitch?

As it redirects you to a secure (SSL) session by default, the login screen may generate a warning from your Web browser or the VNC Java client for two different reasons. First, the CA that has issued the certificate may not yet be recognized as a trusted source by the computer you are using to access the ServSwitch. Second, since the unit could be configured in a number different ways, it is impossible to supply a generic certificate that will match your exact network settings.

Is my data safe?

Yes. The security certificate does not affect encryption effectiveness in any way, nor does it make the ServSwitch any more vulnerable to outside attacks.

Can I prevent the warning from occurring?

Yes. You have two options that may prevent the warning from occurring. First, if the Web browser you are using offers the option to ignore the warning for future visits, the browser will no longer generate a warning if that option is selected. Second, if you install the certificate from the ServSwitch onto the remote computer and if the unit is configured with a domain name ending in .com, .net, .org, .gov, .edu, .us, .ca, .uk, .jp, or .tw (for example, remotecontrol.mydomain.net), then the warning should no longer occur.

C.2 Installing the New Certificate

The following instructions detail how to install the certificate from the ServSwitch onto your local computer (in this case, running Windows XP and Internet Explorer).

1. Open your Web browser and go to the ServSwitch login screen. Click the update security certificate link.

2. When prompted, choose **Open**.

3. A Window will appear that offers information about the certificate. Click on **Install Certificate**.

4. The Certificate Import Wizard will appear. Select **Automatically select the certificate store… (default)** and click **Next**. When the next window appears, click **Finish**.

5. A confirmation dialog will appear asking you if you wish to install the certificate. Click **Yes**.

6. A message should appear saying the import was successful. Click **OK**.

Appendix D. Using an Optional Serial Access Unit (IPMI Supported) with the R-Port

D.1 Background

Using the R-Port on the ServSwitch unit's rear panel, you can add up to 16 serial access units using a specialized daisychain technology. The ServSwitch includes integrated control functionality that allows you to monitor and configure the devices with the RS-232 serial port using the interactive Web interface. To minimize space and infrastructure requirements, the serial access unit uses a single RJ-14 cable (included with the Serial Access Unit, KV9-SRL) to carry both power and the data signal. All configuration settings are stored separately in each attached Serial Access Unit in nonvolatile memory so that they will not be lost in the event of a power outage or disconnection.

D.2 Connecting the Serial Access Unit to the ServSwitch

The RJ-14 cable for attaching the Serial Access Unit (KV9-SRL) via daisychain is similar to a phone cable. For the first computer, connect the RJ-14 cable to the R-port on the ServSwitch unit's rear panel. Then, connect the opposite end of the RJ-14 cable to the Serial Access Unit's RJ-14 port. There are two RJ-14 ports on the Serial Access Unit; choose either one of them. Once you have added the first computer to the ServSwitch by using the Serial Access Unit, you can connect the second computer by using the second Serial Access Unit. Use the second RJ-14 cable to link the first Serial Access Unit and the second one. Then, you can link up to 16 computers.

D.3 Configuring/Viewing the Serial Access Unit Through the Web Interface

Once you have one or more Serial Access Units connected, you will able to configure and manage them through the Web interface. You may need to modify the default settings on the ServSwitch to match your various Serial Access Units' default configuration. Consult the documentation that came with your Serial Access Unit to determine if you need to modify the default settings to complete the installation. To be able to configure your Serial Access Unit, you must be logged in as `admin`. Other users will be able to view which devices are active but cannot configure them.

Once you are logged in, choose **Serial Ports** from the Admin menu on the Home screen in the Web interface. You will be presented with the Serial Consoles Attached menu, and a table with the following headings:

#: You can assign a value (1–99) to each attached serial device to identify the devices so you can manage them. This does not affect the device's configuration or operation in any way.

Name/Description: An identifier for the Serial Access Unit. It's used for administration only.

Baud (bps): This is the device's communication speed. Its setting must match the setting on the device itself. The Serial Access Unit supports all common baud rates between 300 and 115,200 bps.

Mode: Sets the character framing scheme that the ServSwitch will use with the Serial Access Unit. You can choose from the following selections:

- 8N1: Eight bits, no parity, one stop bit (default and most common)
- 7N1/7O1/7E1/7M1/7S1: Seven bits, (none/odd/even/mark/space) parity, one stop bit
- 8N1/8O1/8E1/8M1/8S1: Eight bits, (none/odd/even/mark/space) parity, one stop bit
- 8N2: Eight bits, no parity, two stop bits

Force DCD: Forces the Carrier Detect signal to be active at all times. Normally, DCD becomes active when a new user connects and is dropped when the last user disconnects (a response that is similar to many modems). When active, the device will logout and reset itself if the carrier signal is lost, increasing security. This may not work with all devices and could impair proper operation in some circumstances. The default setting is **Off**.

Console Log: Clicking this link will open a separate Web page that will display the last 200 characters committed to that device's console log. Existing data is overwritten automatically when the 200 character limit is reached.

Connect…: Click on this link to connect to the corresponding device (see **Section D.4**).

You can make as many changes as needed on this menu at one time before applying your changes. Once you are satisfied with the changes you have made, click **Commit changes** to apply the new settings. Click **Refresh** at any time to see an updated list of attached Serial Access Units.

D.4 Advanced Configuration Using the Integrated SSH Shell

In most cases, configuring the ServSwitch to the same settings as the Serial Access Units you are connecting should allow the devices to work with a minimum amount of configuration. However, you can also change the default settings on each Serial Access Unit to fit your preferences and application needs.

If you click the **Connect…** button in Figure 4-14 next to the device you want to configure, two new windows will appear. The smaller window is a login screen; the other is a SSH terminal window. Click on the login window and sign in as `admin` (using the same password as the Web interface) to activate the terminal window. You will see a welcome banner similar to the following:

```
Baud rate: 115200 bps, 8N1
Connected to #1: (none)... (Press Ctrl + Shift + Space for menu).
```

You are now connected to the Serial Access Unit. Commands you type will be echoed on the terminal screen. This simple menu system allows you to change its configuration settings. To access the menu, press **Ctrl + Shift + Space** (in the example below, an underscore represents a space) on the keyboard to access the menu. It will be similar to the following:

```
RS-232 Menu (#1: (none), 115200 bps, 8N1)
  Q - Disconnect
  # - Send break
  H - Hangup line (drop DCD)
  E - Send Ctrl-Shift-_
  L - Low log entries (line buffer)
  1 - Show last 10 log entries
  other - Return to connection
Press key ->
```

To execute the desired command, simply press the corresponding key on the keyboard. You can also execute the command and avoid the menu by pressing the **Ctrl + Shift + Space** key combination quickly and pressing the command's letter. To quit the menu, press **Q** on the keyboard when the menu is active.

D.5 Remote Login via SSH

You can also use a standard SSH client to access the Serial Access Unit options if you don't want to use the Java based SSH client in the Web interface. Simply use your SSH client (several freeware packages are available for download, along with commercial applications) and connect to the ServSwitch unit's IP address using port 22 (default).

Log into the SSH session as `admin` using the same password as the Web interface. At the command prompt, type `connect x` (where `x` is the Serial Access Unit's device number). Or, you can enter `command connect -l` to see a list of active devices.

OPERATING NOTES

- Hardware handshaking (CTS/RTS) is required for speeds exceeding 9600 bps. It is enabled by default on the ServSwitch but may need to be enabled on the other end of the connection. For UNIX systems, the command is:

  ```
  stty -crtscts < /dev/[serial port]
  ```

- Serial Access Units use a simple RS-485 multidrop network running at 115,200 bps. Every Serial Access Unit will not be inputting/outputting data at the same rate at all times. However, since these devices use interactive logins, it is unlikely that all channels would be busy at any one time. Hardware handshaking is used to limit the individual channels' output rates.

- Up to four users may simultaneously log into the same device. All users may type commands at any time, and all users will see the same output.

NOTE

All users have equal access to all channels.

Up to 16 Serial Access Units can be connected at any time.

Plug in and unplug any Serial Access Unit at any time. When reconnected, it will automatically become available after a 15-second initialization period. The Serial Access Unit will retain any log entries while deactivated, but it will not be available to users until you reinitialize it.

D.6 Intelligent Platform Management Interface (IPMI) Function

D.6.1 BACKGROUND

An optional power management feature lets you remotely restart hardware and power the host computer on and off. You can use this feature if the computer supports IPMI (Intelligent Platform Management Interface).

D.6.2 HOST COMPUTER REQUIREMENTS

The host computer must support the IPMI standard version 1.5 to use this option. Most popular server motherboards now support the IPMI standard. To determine if your computer supports this IPMI, consult its documentation for more information.

IPMI lets you configure and control a device on the motherboard called the BMC (Baseboard Management Controller) using a dedicated serial port. Once the computer is configured for IPMI management, the serial port on the host computer is normally reserved by the BIOS solely for that purpose and cannot be accessed or recognized by the operating system. It is therefore unlikely that a serial port provided by an add-in card will be able to act as an IPMI port, so you must use a serial port integrated on the managed computer's motherboard. If the computer you are managing only has a single serial port, you must add an additional port (or ports) via an add-in card if you need a serial port for other purposes (for example, modem). Enabling IPMI support usually requires enabling options in the host computer's BIOS setup software, and the instructions will vary considerably from model to model. Normally, a password will be created by the BIOS that allows you to access the IPMI feature; this password is exclusive to the IPMI feature and does not correspond to a password or account in the host computer's operating system.

D.6.3 IF THE HOST COMPUTER DOES NOT SUPPORT IPMI

If the host computer you are managing with the ServSwitch does not support IPMI, you will need to supply a non-IPMI solution that also works via the serial port and acts as a power concentrator and a power management device.

D.6.4 Activating the IPMI Option

The Serial Access Unit (KV9-SRL) contains the necessary software to use IPMI with the ServSwitch.

You can use either serial port on the ServSwitch to send IPMI access; your choice will dictate the cable type you will use to make the connection. The DTE serial port on the front panel requires a null-modem serial cable.

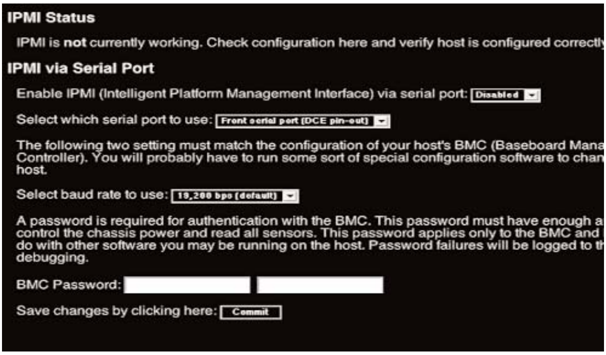
Connect a serial cable's female end to the serial port that's configured for IPMI access on the host computer. Connect the opposite end to the ServSwitch unit's DTE serial port.

D.6.5 Configuring IPMI on the ServSwitch

Once you have connected the IPMI-configured serial port to the ServSwitch and enabled the software option, you can begin to configure IPMI settings through the Web interface.

Log into the Web interface as `admin`. Choose **Serial Ports** from the Admin menu on the Home screen in the Web interface, then select **IPMI/IPMB setup (Intelligent Platform Management)**.

The screen shown in Figure D-1 appears.



IPMI Status

IPMI is **not** currently working. Check configuration here and verify host is configured correctl

IPMI via Serial Port

Enable IPMI (Intelligent Platform Management Interface) via serial port: Disabled

Select which serial port to use: Front serial port (DCE pin-out)

The following two setting must match the configuration of your host's BMC (Baseboard Mana
Controller). You will probably have to run some sort of special configuration software to chan
host.

Select baud rate to use: 19,200 bps (default)

A password is required for authentication with the BMC. This password must have enough a
control the chassis power and read all sensors. This password applies only to the BMC and
do with other software you may be running on the host. Password failures will be logged to th
debugging.

BMC Password:

Save changes by clicking here:

Figure D-1. IPMI Status screen.

Make the following changes to enable IPMI:

- Enable IPMI (Intelligent Platform Management Interface) via the serial port: select **Enabled** from the drop-down menu in Figure D-1.
- From the drop-down menu in Figure D-1, select which serial port to use: select **Front serial port (DTE pinout)** since the ServSwitch has DTE serial port only.

- Select the baud rate between 9600 bps and 115,200 bps based on the configuration on the host computer's IPMI settings.

- BMC Password: Enter the password twice assigned to the BMC in the host computer's BIOS setup software.

NOTE

The selected baud rate should match the host computer's setting. Problems with the BMC password (as well as any other error information) will be recorded in the ServSwitch unit's system log on the Web interface's Status page. If the host computer's BIOS setup allows for multiple levels of security for the BMC, make sure the password you enter on the menu offers sufficient authority to control chassis power and monitor fan status.

Once you have made the necessary changes on this screen, click **Commit** to activate IPMI with the settings you entered.

NOTE

Clicking Commit will cause any active VNC sessions to fail and you will need to re-establish them.

D.6.6 Accessing the Status Screen

The ServSwitch allows you to monitor the host computer's status via IPMI using either the Web interface or the VNC client. The information you will be able to view using the Status screen will depend on the model of host computer being managed. Since IPMI implementations vary widely across manufacturers, the information you are able to see on your status screen may differ from the examples.

NOTE

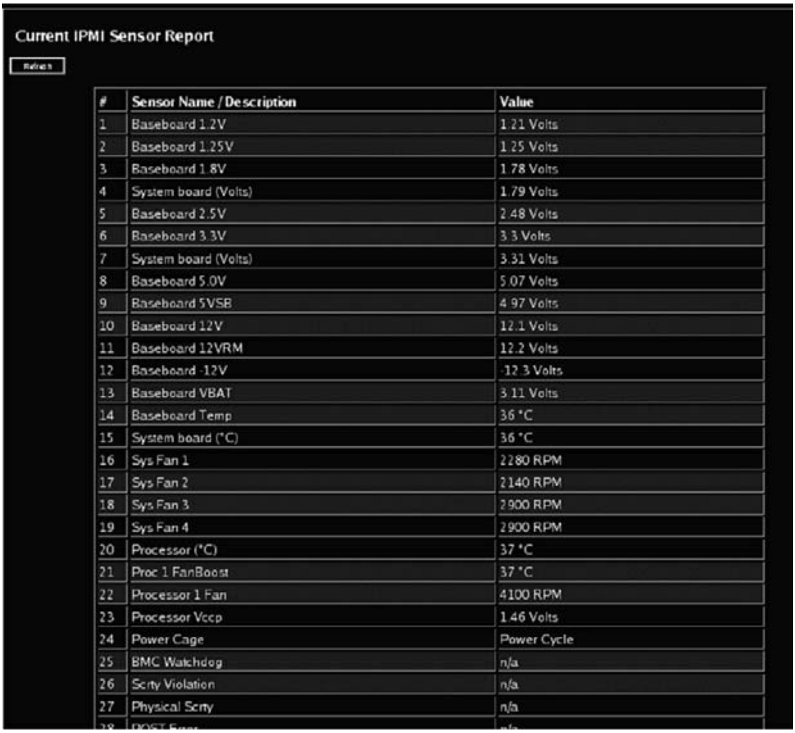
The Status screen will not allow you to make any configuration changes. It's used for monitoring purposes only.

To access the Status (IPMI Sensor Report) screen:

From the Web interface: click **View IMPI sensor report** next to the thumbnail image on the Home screen.

From the VNC interface: click **IMPI** from the bribar at the bottom of the VNC window. Figure D-2 appears.

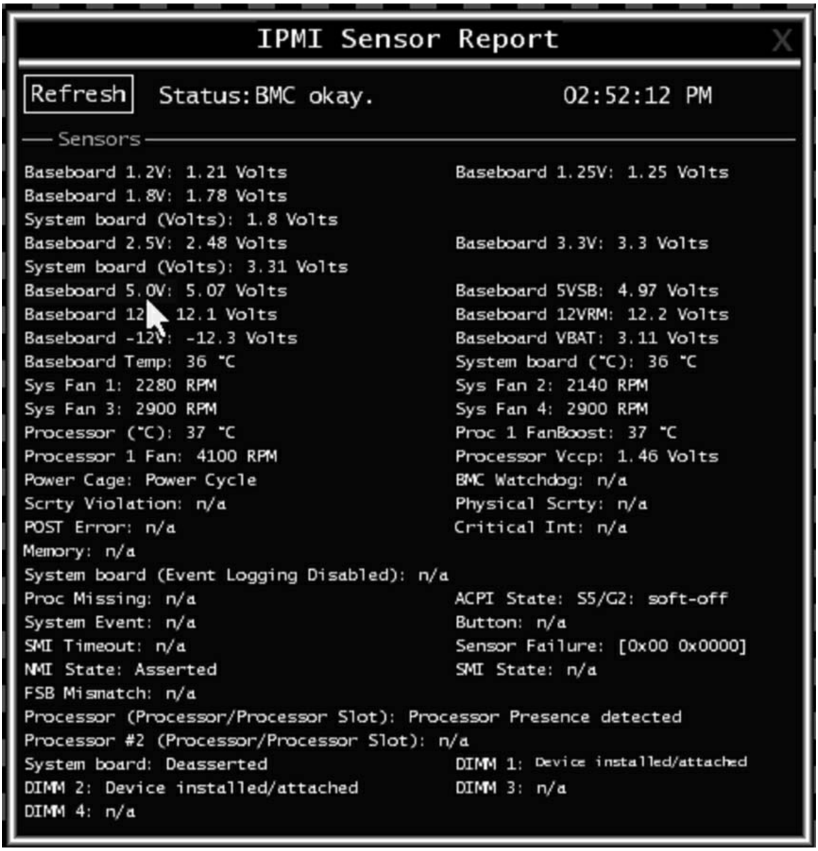
Examples:



Current IPMI Sensor Report

#	Sensor Name / Description	Value
1	Baseboard 1.2V	1.21 Volts
2	Baseboard 1.25V	1.25 Volts
3	Baseboard 1.8V	1.78 Volts
4	System board (Volts)	1.79 Volts
5	Baseboard 2.5V	2.48 Volts
6	Baseboard 3.3V	3.3 Volts
7	System board (Volts)	3.31 Volts
8	Baseboard 5.0V	5.07 Volts
9	Baseboard 5VSB	4.97 Volts
10	Baseboard 12V	12.1 Volts
11	Baseboard 12VRM	12.2 Volts
12	Baseboard -12V	-12.3 Volts
13	Baseboard VBAT	3.11 Volts
14	Baseboard Temp	36 °C
15	System board (°C)	36 °C
16	Sys Fan 1	2280 RPM
17	Sys Fan 2	2140 RPM
18	Sys Fan 3	2900 RPM
19	Sys Fan 4	2900 RPM
20	Processor (°C)	37 °C
21	Proc 1 FanBoost	37 °C
22	Processor 1 Fan	4100 RPM
23	Processor Vccp	1.46 Volts
24	Power Cage	Power Cycle
25	BMC Watchdog	n/a
26	Scrty Violation	n/a
27	Physical Scrty	n/a
28	POST Error	n/a

Figure D-2. VNC status report example #1.



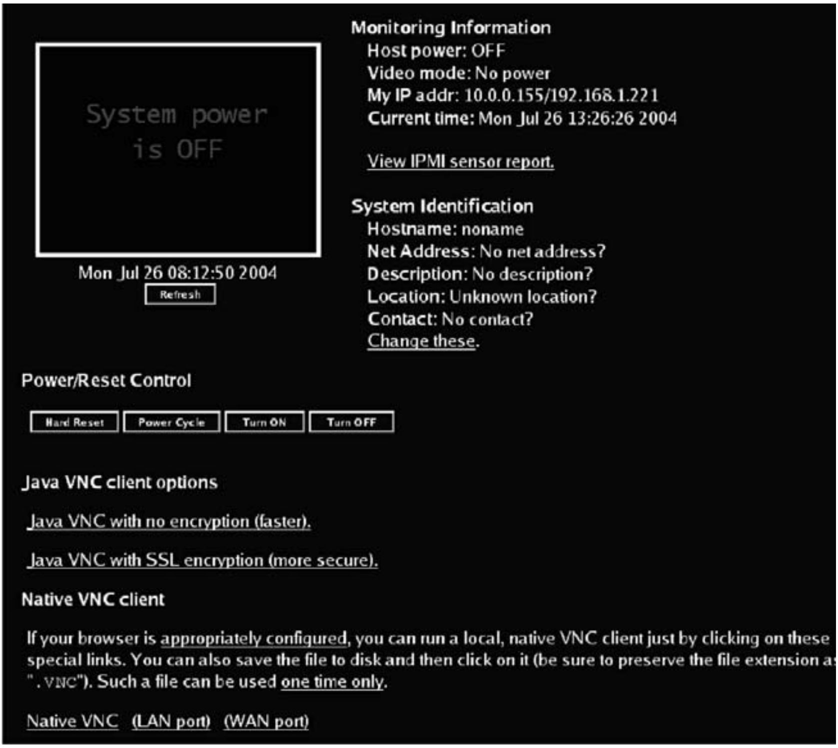
```
Status:BMC okay.                     02:52:12 PM

— Sensors ——————————————————————————————————————————————————————
Baseboard 1.2V: 1.21 Volts                Baseboard 1.25V: 1.25 Volts
Baseboard 1.8V: 1.78 Volts
System board (Volts): 1.8 Volts
Baseboard 2.5V: 2.48 Volts                Baseboard 3.3V: 3.3 Volts
System board (Volts): 3.31 Volts
Baseboard 5.0V: 5.07 Volts                Baseboard 5VSB: 4.97 Volts
Baseboard 12   12.1 Volts                 Baseboard 12VRM: 12.2 Volts
Baseboard -12V: -12.3 Volts               Baseboard VBAT: 3.11 Volts
Baseboard Temp: 36 °C                     System board (°C): 36 °C
Sys Fan 1: 2280 RPM                       Sys Fan 2: 2140 RPM
Sys Fan 3: 2900 RPM                       Sys Fan 4: 2900 RPM
Processor (°C): 37 °C                     Proc 1 FanBoost: 37 °C
Processor 1 Fan: 4100 RPM                 Processor Vccp: 1.46 Volts
Power Cage: Power Cycle                   BMC Watchdog: n/a
Scrty Violation: n/a                      Physical Scrty: n/a
POST Error: n/a                           Critical Int: n/a
Memory: n/a
System board (Event Logging Disabled): n/a
Proc Missing: n/a                         ACPI State: S5/G2: soft-off
System Event: n/a                         Button: n/a
SMI Timeout: n/a                          Sensor Failure: [0x00 0x0000]
NMI State: Asserted                       SMI State: n/a
FSB Mismatch: n/a
Processor (Processor/Processor Slot): Processor Presence detected
Processor #2 (Processor/Processor Slot): n/a
System board: Deasserted                  DIMM 1: Device installed/attached
DIMM 2: Device installed/attached         DIMM 3: n/a
DIMM 4: n/a
```

Figure D-3. VNC status report example #2.

D.6.7 Accessing IPMI Controls

There are two ways to access power controls for the managed computer: through the Home screen on the Web interface or through the bribar during an active VNC session.

Web



Monitoring Information
Host power: OFF
Video mode: No power
My IP addr: 10.0.0.155/192.168.1.221
Current time: Mon Jul 26 13:26:26 2004

View IPMI sensor report.

System Identification
Hostname: noname
Net Address: No net address?
Description: No description?
Location: Unknown location?
Contact: No contact?
Change these.

Mon Jul 26 08:12:50 2004

Power/Reset Control

Java VNC client options

Java VNC with no encryption (faster).

Java VNC with SSL encryption (more secure).

Native VNC client

If your browser is appropriately configured, you can run a local, native VNC client just by clicking on these special links. You can also save the file to disk and then click on it (be sure to preserve the file extension a ".VNC"). Such a file can be used one time only.

Native VNC (LAN port) (WAN port)

Figure D-4. Controls on the Home screen (Web).

Once IPMI is enabled and functioning correctly, a set of controls will appear immediately under the host computer's thumbnail image on the Home screen on the Web interface.

You must be logged in as `admin` to use this feature. From here, you have four options:

- Hard Reset: Equivalent to pressing the Reset button on the managed computer. The computer will restart.
- Power Cycle: Equivalent to pressing the Power button off and on again on the host computer. The computer will power off, pause for a moment, and power on again automatically.

- Turn ON: Powers on the host computer.
- Turn OFF: Powers off the host computer.

VNC

If you are inside an active VNC session and are logged in as `admin`, you can use the bribar to access IPMI features. You have two choices from the bribar:

- Reset: Equivalent to pressing the Reset button on the managed computer. (The computer will restart.)
- ON/OFF: Powers the host computer on or off depending on the current state of the host computer; equivalent to pressing the Power button on the host computer.

NOTE

IPMI may not automatically close the host computer software safely when you issue a Reset or power OFF command. Since these features are equivalent to pressing hardware buttons on the computer itself, the computer will respond in exactly the same way. Always shut down your operating system and application software normally before issuing an IPMI command to avoid data loss or corruption.

Appendix E. Using the Optional Modem Feature

E.1 Background

The modem option allows the ServSwitch to act as an Internet connection server that increases security and flexibility when connecting with the managed computers. Unlike the TCP/IP connection used with the standard Web configuration and VNC clients, the modem creates a one-to-one connection between the ServSwitch and the computer you are using to manage your network. This connection is essentially private, since it bypasses the public Internet completely. This option requires both an external modem (most standard connection protocols are supported) and a dedicated phone line that can be connected to the modem for external access. While it is technically possible to use the modem feature through some PBX systems, this increases the connection's complexity and reduces its performance. For clarity, the instructions presented here assume that the modem is connected to a typical POTS (plain old telephone system) line that is not routed through a phone management system or shared with other devices. If you want to use this feature through a PBX system, you might need additional support from your telecom services provider.

E.2 Connecting a Modem

The ServSwitch works with virtually any Hayes® compatible modem that recognizes the standard AT command set. Some modem manufacturers offer "enterprise" modems that include technology to improve the connections' stability. To determine whether or not you need this type of modem, ask yourself:

1. Is the modem connection mission-critical?

2. Will your telecom infrastructure support such a modem?

3. Will your budget provide a higher-quality modem?

NOTE

Modems that offer “56K” (or 56,000 bps) connections often achieve connection speeds that are far lower than their maximum capabilities. Given the limitations of telecom infrastructure (many locations have yet to implement fully digital switching technology, and still rely on older analog technology for some segments), the maximum “upstream” transfer rate is limited to a maximum of 33,600 bps between two modems; the “downstream” rate is often within a similar range for a typical connection. Therefore, speeds below 56,000 bps do not indicate a problem with the modem or the line but simply reflect the line conditions at the time the connection is made. Use the ServSwitch unit’s rear-panel serial port and a null-modem serial cable for the modem connection.

Place the modem near the ServSwitch and an available telephone jack. The serial cable should have an RJ connector on one end to connect to the line and a DB9 female connector on the other end to connect to the ServSwitch unit’s serial port.

E.2.1 Configuring a Modem Connection on the ServSwitch

Most connections will work appropriately with the ServSwitch unit’s default settings.

Log into the Web interface as `admin`. Choose **Serial Ports** from the Admin menu on the Home screen in the Web interface. Then choose **Modem (PPP) setup**.

The Modem Option menu (not pictured here) will appear.

- To enable modem connections (PPP) via a serial port/modem, select **Enabled**.
- Choose the baud rate to use (affects connection between the ServSwitch and the modem only): select a value from 300 to 115,200 bps.
- Init string: leave as ATE0S0=1&K3.

The baud rate dictates the connection speed between the ServSwitch unit’s serial port and the modem. It does not affect the connection speed between the local and remote modems. (They will negotiate their own connection speed when a connection is made.) For best performance, we recommend that you use the default setting.

The init string is the command (using the standardized Hayes AT command set) that the ServSwitch will send to the modem to activate it. The string included should work with the majority of modems and configures the following connection properties: answer incoming calls on the first ring, enable hardware flow control, and lock the connection speed. Your modem's documentation will describe other potential init strings that you can use to alter the connection properties. For example, you could commit the settings to the modem's nonvolatile memory (NVRAM) or allow the modem to adjust the connection speed for greater stability (and so on). You may want to test the connection with the default init string first before making changes specific to your modem model or situation to simplify the troubleshooting process.

Click the **Commit** button to save your changes and activate the modem feature with the specified settings.

E.2.2 Configuring the Remote Connection

Follow the steps below to configure a typical Windows dialup session to access the ServSwitch unit's modem connection. The instructions here are for a Windows XP configuration; other versions of Windows are similar.

1. Open **My Network Places** from the desktop or the Start menu.
2. Click **View network connections**.
3. Click **Create a new connection** under Network Tasks.
4. The New Connection Wizard window will open. Click **Next**.
5. Select **Connect to the Internet** and click **Next**.
6. Select **Set up my connection manually** and click **Next**.
7. Select **Connect** using a dialup modem and click **Next**.
8. In the space provided under ISP Name, type an appropriate name for the connection. Click **Next**.
9. In the space provided under Phone Number, enter the phone number for the line that the ServSwitch unit's modem is connected to. Add the area code, country code, or other digits needed to access the outside line as required by your phone system. When finished, click **Next**.
10. Select either **Anyone's use** or **My use only** and click **Next**.

11. Beside User name enter the username of any valid user created using the ServSwitch unit's Web interface. Beside Password and Confirm Password, enter the password that the user you entered above uses to access the Web interface.

12. This screen also includes three checkboxes. Uncheck all three checkboxes.

13. Click **Next**.

14. Add a shortcut to the desktop for this connection. Click **Finish**.

You can now use this connection to access the ServSwitch unit's modem. Since you will still log into the unit through the Web interface after establishing a dialup connection, the username on the PPP connection and the username used to access the Web interface do not have to be the same. For security, you might want to create a separate username for dialup access.

The unit will negotiate a PPP connection based on the settings you provided, and no additional scripting or configuration should be required under most circumstances. This is a summary of the settings for use with non Windows operating systems, or other versions of Windows besides XP:

- You must use PPP (Point-to-Point Protocol); the unit supports no other authentication methods.

- The computer making the connection must have TCP/IP installed/enabled on the computer. Use it for the dialup connection.

- Configure the connection to obtain a dynamic IP address.

- Make sure that the username/password matches a user currently configured on the ServSwitch.

- For best performance and to simplify the troubleshooting process, do not use firewall software with the dialup connection.

E.2.3 Accessing the Web Interface

Once a dialup connection has been established, you can access the Web interface or start a VNC session using the following IP address:

```
https://99.99.99.99
```

Log into the Web interface (and/or VNC session) normally. The remote machine (the one you dialed from) is automatically assigned the IP address 99.99.99.100 for the PPP session. You can't modify the remote PC's or the ServSwitch unit's IP addresses. The following TCP/IP port numbers are assigned for a PPP connection, regardless of the settings configured in the Web interface for the LAN port:

```
HTTPS: 443
VNC (clear-text): 5900
VNC (SSL secured): 15900
SSH: 22
```

E.3 Performance Notes

- All images over the PPP connection will be grayscale to conserve bandwidth. If other users are connected while a PPP session is active, their screens will be in grayscale as well. When PPP is inactive, color is automatically re-enabled.

- Some areas of the screen may not be updated as frequently as others, and animations or other auto-updating areas of the screen may appear out-of-focus or "blocky" as a result. Since the area around the mouse pointer refreshes most frequently, hold the pointer over an area to improve its clarity.

- You might want to minimize any unnecessary icons, backgrounds, or other clutter on the managed computer's desktop to make the dial-up connection as efficient as possible.

- To use serial configuration, you must disable the modem feature and reconnect the serial port on the ServSwitch to the managed computer's port.

E.4 Troubleshooting Guide

The following messages will appear in the Web interface's system log on the Status screen. They might help to diagnose problems with the modem configuration.

Message: Starting PPP (for auth) on port…

Description: Modem is connecting and the PPP login process is starting.

Message: Modem hang up. Resetting

Description: The connection has closed or terminated unexpectedly.

Message: Timeout during login process. Giving up

Description: The PPP client connecting over the modem has waited too long to complete the authentication process or supplied an invalid username and/or password.

Message: Modem init chat script failed

Description: The modem did not respond to the initialization string from the ServSwitch. You might need to change the init string or verify the cabling and modem status.

Message: Modem init okay

Description: The modem has responded appropriately to the init string.

Message: PPP startup from client

Description: A PPP authentication has occurred and a session has started.

Message: Phone line rings!

Description: The modem has detected an incoming call.

Message: Modem answers: xxxxxxxxx

Description: The modem reported the connection's speed and protocol. The exact message contents will vary depending on the modem make and model.